Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
GIOVANNI PITRUZZELLA
vom 27. Januar 2022 [1]

Rechtssache C-817/19

Ligue des droits humains
gegen
Ministerrat

(Vorabentscheidungsersuchen der Cour constitutionnelle [Verfassungsgerichtshof, Belgien])

„Vorlage zur Vorabentscheidung – Schutz personenbezogener Daten – Verarbeitung von Fluggastdatensätzen (PNR-Daten) – Verordnung (EU) 2016/679 – Anwendungsbereich – Richtlinie (EU) 2016/681 – Gültigkeit – Charta der Grundrechte der Europäischen Union – Art. 7, 8 und 52 Abs. 1“

Inhaltsverzeichnis

[1] Originalsprache: Französisch.

I. Einleitung

1. Mit dem vorliegenden Vorabentscheidungsersuchen legt der Verfassungsgerichtshof (Belgien) dem Gerichtshof eine Reihe von zehn Fragen nach der Auslegung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden: DSGVO)[2] sowie nach der Gültigkeit und Auslegung der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität (im Folgenden: PNR-Richtlinie)[3] und der Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln (im Folgenden: API-Richtlinie)[4], zur Vorabentscheidung vor. Diese Fragen sind im Rahmen einer von der gemeinnützigen Vereinigung Ligue des droits humains (LDH) erhobenen Klage auf vollständige oder teilweise Nichtigerklärung des Gesetzes vom 25. Dezember 2016 über die Verarbeitung von Passagierdaten (im Folgenden: PNR-Gesetz)[5] aufgeworfen worden, mit dem die PNR-Richtlinie und die API-Richtlinie in belgisches Recht umgesetzt werden.

2. Die Fragen, über die der Gerichtshof in der vorliegenden Rechtssache zu entscheiden haben wird, fügen sich in den Rahmen eines der Hauptdilemmata des zeitgenössischen liberal-demokratischen Konstitutionalismus ein: Wie ist das Verhältnis zwischen Individuum und Gemeinwesen im Zeitalter der Daten zu bestimmen, in dem digitale Technologien die Erhebung, Vorratsspeicherung, Verarbeitung und Auswertung großer Mengen personenbezogener Daten für prädiktive Zwecke ermöglicht haben? Algorithmen, die Analyse von Big Data und künstliche Intelligenz, von denen staatliche Stellen Gebrauch machen, können dazu dienen, die Grundinteressen der Gesellschaft mit einer Effizienz zu fördern und zu schützen, die früher unvorstellbar war: Vom Schutz der öffentlichen Gesundheit zur ökologischen Nachhaltigkeit, von der Bekämpfung des Terrorismus zur Vorbeugung von Kriminalität, insbesondere schwerer Kriminalität. Gleichzeitig können die unterschiedslose Erhebung personenbezogener Daten und die Nutzung digitaler Technologien durch die öffentliche Gewalt

2 ABl. 2016, L 119, S. 1.

3 ABl. 2016, L 119, S. 132.

4 ABl. 2004, L 261, S. 24.

5 *Moniteur belge* vom 25. Januar 2017, S. 12905.

ein digitales Panoptikum schaffen, d. h. eine Staatsmacht, die alles sieht, ohne gesehen zu werden. Eine allwissende Macht, die das Verhalten des Einzelnen kontrollieren und vorhersehen und die gebotenen Maßnahmen ergreifen kann – bis zu dem von Steven Spielberg im Film *Minority Report* erdachten paradoxen Ergebnis, dem Täter eines Delikts, das noch nicht begangen worden ist, vorbeugend die Freiheit zu entziehen. Wie man weiß, hat die Gesellschaft in bestimmten Ländern Vorrang vor dem Individuum und ermöglicht die Verwendung personenbezogener Daten die rechtmäßige Durchführung einer wirksamen Massenüberwachung, mit der die als grundlegend angesehenen öffentlichen Interessen geschützt werden sollen. Umgekehrt stellt der europäische – nationale und supranationale – Konstitutionalismus mit der zentralen Stellung, die dem Individuum und seinen Freiheiten eingeräumt wird, eine große Hürde für den Aufbau einer Gesellschaft der Massenüberwachung dar, vor allem nach der Anerkennung der Grundrechte auf Schutz des Privatlebens und auf Schutz personenbezogener Daten. In welchem Ausmaß kann diese Hürde jedoch errichtet werden, ohne bestimmte Grundinteressen der Gesellschaft – wie etwa die vorstehend beispielhaft angeführten Interessen –, die durchaus verfassungsrechtliche Bezüge haben können, ernsthaft zu beeinträchtigen? Das ist der Kern der Frage nach dem Verhältnis zwischen Individuum und Gemeinwesen in der digitalen Gesellschaft. Eine Frage, die zum einen die Suche nach der heiklen Balance zwischen den Interessen des Gemeinwesens und den Rechten des Einzelnen – wobei von der absoluten Bedeutung ausgegangen wird, die diese im europäischen Verfassungserbe haben – sowie deren Umsetzung und zum anderen das Treffen von Vorkehrungen gegen Missbrauch erforderlich macht. Auch hier befinden wir uns im Bereich der zeitgenössischen Version eines klassischen Themas des Konstitutionalismus, da Menschen, wie *Le Fédéraliste* lapidar festgestellt hat, keine Engel sind und es deshalb rechtlicher Mechanismen bedarf, um die öffentliche Gewalt zu begrenzen und zu kontrollieren.

3. Das sind die Fragen allgemeiner Natur, die sich in den Kontext der vorliegenden Schlussanträge einfügen, wobei sich diese auf die Auslegung des Unionsrechts im Licht der früheren Rechtsprechung des Gerichtshofs unter Verwendung etablierter Techniken beschränken müssen, zu denen die Technik der unionsrechtskonformen Auslegung gehört. Eine Technik, auf die in den vorliegenden Schlussanträgen oft zurückgegriffen werden soll, wenn das rechtlich möglich erscheint – mit dem Ziel, die aus verfassungsrechtlicher Sicht notwendige Balance zwischen den öffentlichen Zwecken, die dem System für die Übermittlung, Erhebung und Verarbeitung von Fluggastdatensätzen (im Folgenden: PNR-Daten) zugrunde liegen, und den in den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) niedergelegten Rechte zu finden.

II. Rechtlicher Rahmen

A. Unionsrecht

1. Charta

4. Art. 7 der Charta lautet: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."

5. In Art. 8 der Charta heißt es:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

6. Gemäß Art. 52 Abs. 1 der Charta muss „[j]ede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten … gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen".

2. DSGVO

7. Art. 2 Abs. 2 Buchst. d der DSGVO schließt die Verarbeitung personenbezogener Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" vom Anwendungsbereich dieser Verordnung aus.

8. In Art. 23 Abs. 1 Buchst. d der DSGVO heißt es:

„Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

…

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit".

3. PNR-Richtlinie

9. Ich werde im Folgenden nur einen kurzen Überblick über die Funktionsweise des mit der PNR-Richtlinie geschaffenen Systems geben. Weitere Einzelheiten zum Inhalt der Bestimmungen der PNR-Richtlinie, die für die auf die Vorlagefragen zu gebende Antwort relevant ist, sollen im Verlauf der rechtlichen Würdigung geliefert werden.

10. Gemäß ihrem Art. 1 wird mit der PNR-Richtlinie, die auf der Grundlage von Art. 82 Abs. 1 Buchst. d AEUV und Art. 87 Abs. 2 Buchst. a AEUV erlassen worden ist, auf der Ebene der Europäischen Union ein System für die Übermittlung von PNR-Daten zu Fluggästen von

Drittstaatsflügen[6] durch Fluggesellschaften sowie für die Erhebung, Verarbeitung und Speicherung dieser Daten durch die zuständigen Behörden der Mitgliedstaaten zum Zwecke der Bekämpfung von Terrorismus und schwerer Kriminalität eingeführt.

11. Gemäß Art. 3 Nr. 5 dieser Richtlinie bezeichnet der Ausdruck „Fluggastdatensatz“ oder „PNR-Daten“ einen „Datensatz mit den für die Reise notwendigen Angaben zu jedem einzelnen Fluggast, die die Bearbeitung und Überprüfung der von einer Person oder in ihrem Namen getätigten Reservierungen für jede Reise durch die buchenden und beteiligten Fluggesellschaften ermöglichen, unabhängig davon, ob er in Buchungssystemen, Abfertigungssystemen (Departure Control Systems) zum Einchecken von Passagieren auf Flüge[] oder gleichwertigen Systemen, die die gleichen Funktionen bieten, enthalten ist“.

12. In Anhang I der PNR-Richtlinie (im Folgenden: Anhang I) sind die von Fluggesellschaften erhobenen PNR-Daten aufgeführt, die im Sinne und nach den Modalitäten von Art. 8 dieser Richtlinie übermittelt werden.

13. Anhang II der PNR-Richtlinie (im Folgenden: Anhang II) enthält eine Liste der strafbaren Handlungen, die „schwere Kriminalität“ im Sinne von Art. 3 Nr. 9 dieser Richtlinie darstellen.

14. Art. 2 der PNR-Richtlinie sieht für die Mitgliedstaaten die Möglichkeit vor, zu entscheiden, diese Richtlinie auch auf „Flüge innerhalb der Europäischen Union (EU-Flüge)“[7] oder einige von ihnen, die für die Verfolgung der Ziele der Richtlinie für „erforderlich“ gehalten werden, anzuwenden.

15. Gemäß Art. 4 Abs. 1 der PNR-Richtlinie errichtet oder benennt [j]eder Mitgliedstaat … eine für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständige Behörde oder eine Abteilung einer solchen Behörde, die als seine PNR-Zentralstelle handelt“. Nach Abs. 2 Buchst. a dieses Artikels ist die PNR-Zentralstelle u. a. verantwortlich für die Erhebung der PNR-Daten bei Fluggesellschaften, für die Speicherung und Verarbeitung dieser Daten sowie die Übermittlung dieser Daten oder der Ergebnisse ihrer Verarbeitung an die zuständigen Behörden nach Art. 7 der PNR-Richtlinie. Gemäß Art. 7 Abs. 2 sind diese Behörden „diejenigen Behörden, die für die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von terroristischen Straftaten oder schwerer Kriminalität zuständig sind“[8].

6 Gemäß Art. 3 Nr. 2 der PNR-Richtlinie ist ein „Drittstaatsflug“ „jede[r] Linien- oder Gelegenheitsflug einer Fluggesellschaft, der von einem Drittstaat aus startet und das Hoheitsgebiet eines Mitgliedstaats zum Ziel hat, oder der vom Hoheitsgebiet eines Mitgliedstaats aus startet und einen Drittstaat zum Ziel hat, wobei in beiden Fällen Flüge mit Zwischenlandungen im Hoheitsgebiet von Mitgliedstaaten oder Drittstaaten eingeschlossen sind“.

7 Gemäß Art. 3 Nr. 3 der PNR-Richtlinie ist ein „EU-Flug“ „jede[r] Linien- oder Gelegenheitsflug einer Fluggesellschaft, der vom Hoheitsgebiet eines Mitgliedstaats aus startet und das Hoheitsgebiet eines oder mehrerer anderer Mitgliedstaaten zum Ziel hat, ohne Zwischenlandungen im Hoheitsgebiet eines Drittstaats“.

8 Art. 7 Abs. 1 der PNR-Richtlinie sieht vor, dass jeder Mitgliedstaat eine Liste der zuständigen Behörden erstellt, die berechtigt sind, zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität PNR-Daten oder die Ergebnisse der Verarbeitung dieser Daten von den PNR-Zentralstellen anzufordern oder entgegenzunehmen, um sie einer weiteren Prüfung zu unterziehen oder um geeignete Maßnahmen zu veranlassen.“ Diese Liste ist 2018 von der Kommission veröffentlicht worden (ABl. 2018, C 194, S. 1, berichtigt in ABl. 2020, C 366, S. 55).

16. In Art. 6 Abs. 1 Satz 2 der PNR-Richtlinie heißt es: „Wenn die von Fluggesellschaften übermittelten PNR-Daten andere als die in Anhang I genannten Daten beinhalten, werden diese Daten von der PNR-Zentralstelle unmittelbar nach ihrem Eingang dauerhaft gelöscht." Abs. 2 dieses Artikels hat folgenden Wortlaut:

„(2) Die PNR-Zentralstelle verarbeitet PNR-Daten ausschließlich zu folgenden Zwecken:

a) Überprüfung von Fluggästen vor ihrer planmäßigen Ankunft in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat, um diejenigen Personen zu ermitteln, die von den zuständigen Behörden gemäß Artikel 7 und gegebenenfalls – im Einklang mit Artikel 10 – von Europol genauer überprüft werden müssen, da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind;

b) im Einzelfall Beantwortung von auf einer hinreichenden Grundlage gebührend begründeten Anfragen zuständiger Behörden hinsichtlich der Zurverfügungstellung und Verarbeitung von PNR-Daten in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität[] und der Zurverfügungstellung der Ergebnisse dieser Verarbeitung an die zuständigen Behörden oder gegebenenfalls an Europol, und

c) Analyse von PNR-Daten zwecks Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind".

17. Art. 12 der PNR-Richtlinie enthält Bestimmungen über die Speicherung von PNR-Daten.

18. Art. 5 der PNR-Richtlinie sieht vor, dass die PNR-Zentralstelle einen Datenschutzbeauftragten ernennt, der für die Überwachung der Verarbeitung der PNR-Daten und die Umsetzung der maßgeblichen Sicherheitsvorkehrungen zuständig ist. Außerdem ist jeder Mitgliedstaat gemäß Art. 15 dieser Richtlinie verpflichtet, die nationale Kontrollstelle gemäß Art. 25 des Rahmenbeschlusses 2008/977/JI[9], ersetzt durch die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: Polizei-Richtlinie)[10], mit der Kontrolle hinsichtlich der Anwendung der zur Umsetzung der Richtlinie erlassenen nationalen Vorschriften in seinem Hoheitsgebiet zu beauftragen. Diese Stelle, die ihre Aufgaben erfüllt, um die Grundrechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu schützen[11], ist u. a. für die Behandlung von Beschwerden betroffener Personen, die Untersuchung der Angelegenheit und Unterrichtung der betroffenen Personen über den Fortgang und das Ergebnis der Beschwerde innerhalb einer angemessenen Frist einerseits und die Prüfung der Rechtmäßigkeit der Datenverarbeitung sowie die Durchführung von Ermittlungen, Inspektionen und Audits gemäß nationalem Recht entweder aus eigener Initiative oder aufgrund einer Beschwerde andererseits verantwortlich[12].

9 Rahmenbeschluss des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. 2008, L 350, S. 60).

10 ABl. 2016, L 119, S. 89. Art. 25 des Rahmenbeschlusses 2008/977/JI ist durch Art. 41 der Polizei-Richtlinie ersetzt worden.

11 Vgl. Art. 15 Abs. 2 der PNR-Richtlinie.

12 Vgl. Art. 15 Abs. 3 Buchst. a und b der PNR-Richtlinie.

4. Weitere einschlägige Rechtsakte der Union

19. Der rechtliche Rahmen der vorliegenden Rechtssache wird durch die API-Richtlinie und die Polizei-Richtlinie vervollständigt. Aus Gründen der Lesbarkeit der vorliegenden Schlussanträge soll der Inhalt der einschlägigen Bestimmungen dieser Rechtsakte nur insoweit dargelegt werden, als sich das für die Behandlung der sie betreffenden Fragen oder ganz allgemein für die Zwecke der rechtlichen Würdigung als erforderlich erweist.

B. Belgisches Recht

20. Nach Art. 22 der belgischen Verfassung hat „[j]eder … ein Recht auf Achtung vor seinem Privat- und Familienleben, außer in den Fällen und unter den Bedingungen, die durch Gesetz festgelegt sind".

21. Gemäß seinem Art. 2 werden mit dem PNR-Gesetz die API-Richtlinie und die PNR-Richtlinie sowie teilweise die Richtlinie 2010/65/EU [13] umgesetzt.

22. Nach seinem Art. 3 § 1 bestimmt das PNR-Gesetz „die Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen in Bezug auf die Übermittlung von Daten zu Passagieren, die in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet befördert werden". Gemäß Art. 4 Nrn. 1 und 2 dieses Gesetzes versteht man unter „Beförderungsunternehmen" „eine natürliche oder juristische Person, die gewerblich die Beförderung von Personen auf dem Luft-, See-, Eisenbahn- oder Landweg durchführt", und unter „Reiseunternehmen" „einen Reiseveranstalter oder -vermittler im Sinne des Gesetzes vom 16. Februar 1994 zur Regelung des Reiseveranstaltungsvertrags und des Reisevermittlungsvertrags".

23. Art. 8 des PNR-Gesetzes sieht vor:

„§ l. Die Passagierdaten werden zu folgenden Zwecken verarbeitet:

1. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 90*ter* § 2 … Nr. 7, 8, 11, 14, 17 bis [19] … und § 3 des Strafprozessgesetzbuches erwähnten Straftaten,

2. Ermittlung und Verfolgung, einschließlich Vollstreckung von Strafen oder freiheitsbeschränkenden Maßnahmen, in Bezug auf die in Artikel 196, was die Fälschung authentischer und öffentlicher Urkunden betrifft, 198, 199, 199*bis*, 207, 213, 375 und 505 des Strafgesetzbuches erwähnten Straftaten,

3. Verhinderung schwerer Störungen der öffentlichen Sicherheit im Rahmen der gewalttätigen Radikalisierung durch Beobachtung der Phänomene und Gruppierungen gemäß Artikel 44/5 § 1 Nr. 2 und 3 und § 2 des Gesetzes vom 5. August 1992 über das Polizeiamt,

[13] Richtlinie des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG (ABl. 2010, L 283, S. 1).

4. Beaufsichtigung der in den Artikeln 7 Nr. 1 und 3/1 und 11 § 1 Nr. 1 bis 3 und 5 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste[14] erwähnten Aktivitäten,

5. Ermittlung und Verfolgung der Straftaten, erwähnt in Artikel 220 § 2 des allgemeinen Gesetzes vom 18. Juli 1977 über Zölle und Akzisen, in Artikel 45 Absatz 3 des Gesetzes vom 22. Dezember 2009 über die allgemeine Akzisenregelung …

§ 2. Die Passagierdaten werden unter den in Kapitel 11 erwähnten Bedingungen ebenfalls verarbeitet, um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen."

24. Art. 9 des PNR-Gesetzes enthält eine Liste der Daten, die übermittelt werden. Diese Daten entsprechen den in Anhang I aufgeführten Daten.

25. Art. 18 des PNR-Gesetzes lautet: „Passagierdaten werden höchstens fünf Jahre ab ihrer Speicherung in der Passagierdatenbank aufbewahrt. Am Ende dieser Frist werden sie vernichtet."

26. Art. 19 dieses Gesetzes sieht vor: „Nach Ablauf einer sechsmonatigen Frist ab der Speicherung der Passagierdaten in der Passagierdatenbank werden alle Passagierdaten durch Unkenntlichmachung [von] Datenelemente[n] … depersonalisiert[.]"

27. Art. 24 des PNR-Gesetzes bestimmt:

„§ 1. Die Passagierdaten werden im Hinblick auf die Durchführung einer Vorabüberprüfung der Passagiere vor ihrer Ankunft im nationalen Hoheitsgebiet, ihrer Abreise aus dem nationalen Hoheitsgebiet oder ihrer Durchreise durch das nationale Hoheitsgebiet verarbeitet, um diejenigen Personen zu ermitteln, die genauer überprüft werden müssen.

§ 2. Im Rahmen der Zwecke, die in Artikel 8 § 1 Nr. 1, 4 und 5 erwähnt sind oder sich auf Bedrohungen beziehen, die in den Artikeln 8 Nr. 1 Buchstabe a), b), c), d), f), g) und 11 § 2 des Grundlagengesetzes vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste aufgeführt sind, beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und:

1. den Datenbanken, die von den zuständigen Diensten verwaltet werden oder die ihnen im Rahmen ihrer Aufträge unmittelbar zur Verfügung stehen oder zugänglich sind, oder Personenlisten, die von den zuständigen Diensten im Rahmen ihrer Aufträge erstellt werden,

2. den Überprüfungskriterien, die von der PNR-Zentralstelle im Voraus festgelegt sind und in Artikel 25 erwähnt sind.

§ 3. Im Rahmen der in Artikel 8 § 1 Nr. 3 erwähnten Zwecke beruht die Vorabüberprüfung der Passagiere auf einem Treffer aus einer Korrelation zwischen den Passagierdaten und den in § 2 Nr. 1 erwähnten Datenbanken.

…"

14 *Moniteur belge* vom 18. Dezember 1998, S. 40312.

28. Art. 25 des PNR-Gesetzes übernimmt den Inhalt von Art. 6 Abs. 4 der PNR-Richtlinie.

29. Kapitel 11 des PNR-Gesetzes enthält Vorschriften über die Verarbeitung der Passagierdaten im Hinblick auf eine Verbesserung der Grenzkontrolle und die Bekämpfung der illegalen Einwanderung. Diese Vorschriften stellen die Umsetzung der API-Richtlinie in belgisches Recht dar.

30. Art. 44 des PNR-Gesetzes sieht vor, dass die PNR-Zentralstelle einen Datenschutzbeauftragten innerhalb des Föderalen Öffentlichen Dienstes Inneres bestimmt. Die Kontrolle hinsichtlich der Anwendung der Bestimmungen des PNR-Gesetzes wird vom Ausschuss für den Schutz des Privatlebens ausgeübt.

31. Mit Art. 51 des PNR-Gesetzes wird das Grundlagengesetz vom 30. November 1998 über die Nachrichten- und Sicherheitsdienste durch Einfügung eines Art. 16/3 mit folgendem Wortlaut abgeändert:

„§ 1. Die Nachrichten- und Sicherheitsdienste können im Interesse der Ausübung ihrer Aufträge und ordnungsgemäß begründet beschließen, auf die in Artikel 7 des [PNR-Gesetzes] erwähnten Passagierdaten zuzugreifen.

§ 2. Der in § 1 erwähnte Beschluss wird von einem Dienstleiter gefasst und der in Kapitel 7 des vorerwähnten Gesetzes erwähnten PNR-Zentralstelle schriftlich übermittelt. Der Beschluss wird zusammen mit seiner Begründung dem Ständigen Ausschuss N notifiziert.

Der Ständige Ausschuss N verbietet den Nachrichten- und Sicherheitsdiensten, die gesammelten Daten unter Bedingungen zu benutzen, die die gesetzlichen Bedingungen nicht einhalten.

Der Beschluss kann eine Gesamtheit von Daten in Bezug auf eine spezifische nachrichtendienstliche Untersuchung betreffen. In diesem Fall wird dem Ständigen Ausschuss N einmal pro Monat die Liste der Abfragen der Passagierdaten übermittelt."

C. Ausgangsrechtsstreit, Vorlagefragen und Verfahren vor dem Gerichtshof

32. Mit einer an den Verfassungsgerichtshof gerichteten Klageschrift vom 24. Juli 2017 erhob die LDH Klage auf vollständige oder teilweise Nichtigerklärung des PNR-Gesetzes. Zur Stützung ihrer Klage machte sie zwei Klagegründe geltend.

33. Mit ihrem ersten Klagegrund eines Verstoßes gegen Art. 22 der belgischen Verfassung in Verbindung mit Art. 23 der DSGVO, den Art. 7, 8 und 52 Abs. 1 der Charta sowie Art. 8 der am 4. November 1950 in Rom unterzeichneten Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden: EMRK) vertritt die LDH die Ansicht, das angefochtene Gesetz verstoße hinsichtlich seines Anwendungsbereichs und der genannten Datenkategorien, der mit ihm eingeführten Datenverarbeitungen, seiner Zwecke sowie der Aufbewahrungsdauer der Daten gegen den Grundsatz der Verhältnismäßigkeit. Sie trägt insbesondere vor, dass die Definition der PNR-Daten zu weit sei und zur Preisgabe sensibler Daten führen könne und dass die in diesem Gesetz enthaltene Definition des Begriffs „Passagier" eine systematische und nicht zielgerichtete Verarbeitung der Daten aller betroffenen Fluggäste ermögliche. Außerdem würden im PNR-Gesetz weder die Art und die Modalitäten der *Pre-Screening*-Methode der Passagierdatenbanken noch die Kriterien festgelegt, die als „Indikatoren für die Bedrohung" dienten. Schließlich überschreite das PNR-Gesetz die Grenzen

des absolut Notwendigen in dem Sinne, dass es Zwecke der Verarbeitung von PNR-Daten verfolge, die über die in der PNR-Richtlinie zugelassenen Zwecke hinausgingen; auch sei die Aufbewahrungsdauer von fünf Jahren für PNR-Daten unverhältnismäßig. Mit ihrem hilfsweise vorgebrachten zweiten Klagegrund, mit dem ein Verstoß gegen Art. 22 der belgischen Verfassung in Verbindung mit Art. 3 Abs. 2 EUV und Art. 45 der Charta geltend gemacht wird, greift die LDH die Bestimmungen von Kapitel 11 des PNR-Gesetzes an, mit denen die API-Richtlinie umgesetzt wird.

34. Der Ministerrat des Königreichs Belgien wendet sich als Streithelfer vor dem Verfassungsgerichtshof gegen die Klage der LDH und bestreitet sowohl die Zulässigkeit als auch die Begründetheit der beiden zu ihrer Stützung vorgebrachten Klagegründe.

35. Der Verfassungsgerichtshof stellt seinerseits folgende Erwägungen an.

36. In Bezug auf den ersten Klagegrund fragt er sich zunächst, ob die Definition der PNR-Daten in Anhang I hinreichend klar und präzise ist. Die Beschreibung bestimmter Daten habe beispielhaften und nicht erschöpfenden Charakter. Sodann habe die Definition des Begriffs „Fluggast“ in Art. 3 Nr. 4 der PNR-Richtlinie die Erhebung, Übermittlung, Verarbeitung und Speicherung der PNR-Daten jeder beförderten oder zu befördernden und in der Passagierliste eingetragenen Person zur Folge, unabhängig davon, ob ein begründeter Verdacht bestehe, dass die betreffende Person eine Straftat begangen habe oder in naher Zukunft begehen werde oder für eine Straftat verurteilt worden sei. Bezüglich der Verarbeitungen der PNR-Daten weist er darauf hin, dass diese systematisch Gegenstand einer Vorabüberprüfung seien, bei der die PNR-Daten aller Fluggäste mit Datenbanken oder im Voraus festgelegten Kriterien abgeglichen würden, um Übereinstimmungen festzustellen. Gleichwohl stellt der Verfassungsgerichtshof klar, dass die Kriterien zwar spezifisch, zuverlässig und nicht diskriminierend sein müssten, es ihm aber technisch unmöglich erscheine, die im Voraus festgelegten Kriterien für die Bestimmung von Risikoprofilen weiter zu definieren. In Bezug auf die Frist für die Speicherung der PNR-Daten gemäß Art. 12 Abs. 1 der PNR-Richtlinie, wonach diese Daten für einen Zeitraum von fünf Jahren vorgehalten werden können, vertritt das vorlegende Gericht die Auffassung, die PNR-Daten würden aufbewahrt, ohne die Frage zu berücksichtigen, ob die betreffenden Fluggäste im Rahmen der Vorabüberprüfung eine Gefahr für die öffentliche Sicherheit darstellen könnten oder nicht. Unter diesen Umständen fragt sich das vorlegende Gericht, ob in Anbetracht der u. a. aus dem Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a.[15], sowie dem Gutachten 1/15 (PNR-Abkommen EU–Kanada) vom 26. Juli 2017[16] hervorgegangenen Rechtsprechung davon ausgegangen werden kann, dass das mit der PNR-Richtlinie geschaffene System für die Erhebung, Übermittlung, Verarbeitung und Aufbewahrung von PNR-Daten nicht die Grenzen des absolut Notwendigen überschreitet. In diesem Zusammenhang fragt sich der Verfassungsgerichtshof auch, ob die PNR-Richtlinie einer nationalen Regelung wie der sich aus Art. 8 Abs. 1 Nr. 4 des PNR-Gesetzes ergebenden entgegensteht, die eine Verarbeitung der PNR-Daten zu einem anderen als den in der Richtlinie vorgesehenen Zwecken gestattet. Er fragt sich schließlich, ob die PNR-Zentralstelle als „andere nationale Behörde“ angesehen werden kann, die gemäß Art. 12 Abs. 3 Buchst. b Ziff. ii der PNR-Richtlinie nach einer Frist von sechs Monaten die Offenlegung der vollständigen PNR-Daten gestatten könnte. Zum zweiten Klagegrund stellt das vorlegende Gericht fest, dass sich dieser gegen Art. 3 Abs. 1, Art. 8 Abs. 2 sowie die Art. 28 bis 31 des PNR-Gesetzes richte, in denen die Erhebung und Verarbeitung von Passagierdaten zur Bekämpfung der illegalen Einwanderung und zur Verbesserung der Grenzkontrollen geregelt seien. Das vorlegende

15 C-203/15 und C-698/15, im Folgenden: Urteil Tele2 Sverige, EU:C:2016:970.

16 Im Folgenden: Gutachten 1/15, EU:C:2017:592.

Gericht weist darauf hin, dass das PNR-Gesetz nach der erstgenannten Vorschrift Flüge in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet und durch das nationale Hoheitsgebiet erfasse, und stellt klar, dass der nationale Gesetzgeber „EU-Flüge“ in den Anwendungsbereich des Gesetzes einbezogen habe, um „ein umfassenderes Bild der Bewegungen von Passagieren zu erhalten, die eine potenzielle Bedrohung für die [Sicherheit innerhalb der Union] und [die] nationale Sicherheit darstellen“, wobei es sich auf die Möglichkeit stützt, die in Art. 2 der PNR-Richtlinie in Verbindung mit deren zehntem Erwägungsgrund vorgesehen ist.

37. In diesem Kontext hat der Verfassungsgerichtshof beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Ist Art. 23 der [DSGVO] in Verbindung mit Art. 2 Abs. 2 Buchst. d dieser Verordnung so auszulegen, dass er auf einzelstaatliche Rechtsvorschriften wie das [PNR-Gesetz], mit dem die [PNR-Richtlinie] sowie die [API-Richtlinie] und die Richtlinie 2010/65 umgesetzt werden, anwendbar ist?

2. Ist Anhang I … mit den Art. 7, 8 und 52 Abs. 1 der [Charta] in dem Sinne vereinbar, dass die darin aufgeführten Daten sehr weitgehend sind – insbesondere die in Nr. 18 [dieses Anhangs I] erwähnten Daten, die über die in Art. 3 Abs. 2 der [API-Richtlinie] erwähnten Daten hinausgehen – insofern sie zusammengenommen sensible Daten offenlegen könnten und so über das „absolut Notwendige“ hinausgehen könnten?

3. Sind die Nrn. 12 und 18 des Anhangs I … mit den Art. 7, 8 und 52 Abs. 1 der [Charta] vereinbar, insofern unter Berücksichtigung des Wortes „einschließlich“ die dort aufgeführten Daten in beispielhafter und nicht erschöpfender Weise genannt werden, was somit gegen die Anforderung der Präzision und Klarheit der Regeln, die einen Eingriff in das Recht auf Achtung des Privatlebens und das Recht auf Schutz personenbezogener Daten nach sich ziehen, verstoßen könnte?

4. Sind Art. 3 Nr. 4 der [PNR-Richtlinie] und Anhang I … mit den Art. 7, 8 und 52 Abs. 1 der [Charta] vereinbar, insofern das System zur allgemeinen Erhebung, Übermittlung und Verarbeitung von Passagierdaten, das mit diesen Bestimmungen eingeführt wird, auf jede Person abzielt, die das betreffende Beförderungsmittel benutzt, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von dieser Person eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

5. Ist Art. 6 der [PNR-Richtlinie] in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der [Charta] dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das als Verarbeitungszweck der PNR-Daten die Beaufsichtigung der erwähnten Aktivitäten durch die Nachrichten- und Sicherheitsdienste zulässt und so diesen Zweck in die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität aufnimmt?

6. Ist Art. 6 der [PNR-Richtlinie] mit den Art. 7, 8 und 52 Abs. 1 der [Charta] vereinbar, insofern die in ihm geregelte Vorabüberprüfung durch eine Korrelation mit Datenbanken und im Voraus festgelegten Kriterien systematisch und allgemein auf die Passagierdaten angewandt wird, unabhängig von einem objektiven Anhaltspunkt für die Annahme, dass von diesen Fluggästen eine Gefahr für die öffentliche Sicherheit ausgehen könnte?

7. Kann der in Art. 12 Abs. 3 der [PNR-Richtlinie] erwähnte Ausdruck „andere nationale Behörde, die … zuständig ist“ dahin ausgelegt werden, dass er sich auf die PNR-Zentralstelle bezieht, die durch das [PNR-Gesetz] geschaffen wurde und die somit den Zugriff auf die PNR-Daten nach einer sechsmonatigen Frist im Rahmen von gezielten Recherchen gestatten dürfte?

8. Ist Art. 12 der [PNR-Richtlinie] in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der [Charta] dahin auszulegen, dass er einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das eine allgemeine Aufbewahrungsdauer für die Daten von fünf Jahren vorsieht, ohne eine Unterscheidung danach vorzunehmen, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Fluggäste ein Risiko für die öffentliche Sicherheit darstellen können oder nicht?

9. a) Ist die [API-Richtlinie] mit Art. 3 Abs. 2 [EUV] und mit Art. 45 der [Charta] vereinbar, insofern die Pflichten, die sie einführt, für Flüge innerhalb der … Union gelten?

   b) Ist die [API-Richtlinie] in Verbindung mit Art. 3 Abs. 2 [EUV] und mit Art. 45 der [Charta] dahin auszulegen, dass sie einzelstaatlichen Rechtsvorschriften wie dem angefochtenen Gesetz entgegensteht, das zum Zwecke der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrollen ein System zur Erhebung und Verarbeitung der Daten „zu den in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet“ beförderten Passagieren gestattet, was indirekt eine Wiedereinführung von Kontrollen an den Binnengrenzen bedeuten könnte?

10. Könnte der Verfassungsgerichtshof, falls er auf der Grundlage der Antworten auf die vorstehenden Vorabentscheidungsfragen zu dem Schluss gelangen sollte, dass das angefochtene Gesetz, mit dem insbesondere die [PNR-Richtlinie] umgesetzt wird, gegen eine oder mehrere der Verpflichtungen verstößt, die sich aus den in diesen Fragen genannten Bestimmungen ergeben, die Folgen des [PNR-Gesetzes] vorläufig aufrechterhalten, um eine Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch [dieses] Gesetz angestrebten Ziele benutzt werden können?

38. Die LDH, die belgische, die tschechische, die dänische, die deutsche, die estnische, die irische, die spanische, die französische, die zyprische, die lettische, die niederländische, die österreichische, die polnische und die finnische Regierung sowie das Europäische Parlament, der Rat der Europäischen Union und die Europäische Kommission haben gemäß Art. 23 der Satzung des Gerichtshofs der Europäischen Union schriftliche Erklärungen eingereicht. Nach Art. 24 der Satzung des Gerichtshofs der Europäischen Union sind die Kommission, der Europäische Datenschutzbeauftragte (EDSB) und die Agentur der Europäischen Union für Grundrechte (FRA) aufgefordert worden, schriftlich auf Fragen des Gerichtshofs zu antworten. Eine mündliche Verhandlung hat am 13. Juli 2021 stattgefunden.

III. Würdigung

A. Zur ersten Vorlagefrage

39. Mit seiner ersten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof wissen, ob Art. 2 Abs. 2 Buchst. d der DSGVO dahin auszulegen ist, dass diese Verordnung, insbesondere ihr Art. 23 Abs. 1, wonach durch Rechtsvorschriften der Union oder der Mitgliedstaaten die Pflichten und Rechte gemäß der Verordnung im Wege von Gesetzgebungsmaßnahmen aus abschließend aufgeführten Gründen beschränkt werden können, für Datenverarbeitungen auf der Grundlage nationaler Rechtsvorschriften wie des PNR-Gesetzes gilt, mit dem die PNR-Richtlinie sowie die API-Richtlinie und die Richtlinie 2010/65 in innerstaatliches Recht umgesetzt werden.

40. Art. 2 Abs. 2 der DSGVO sieht Ausnahmen vom Anwendungsbereich dieser Verordnung vor, der in deren Art. 2 Abs. 1 [17] sehr weit definiert wird [18]. Als Abweichungen von der Anwendung einer Regelung für die Verarbeitung personenbezogener Daten, die die Grundfreiheiten beeinträchtigen könnte, sind diese Ausnahmen eng auszulegen [19].

41. Art. 2 Abs. 2 Buchst. d der DSGVO enthält u. a. eine Ausschlussklausel, wonach diese Verordnung auf die Verarbeitung personenbezogener Daten „durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ keine Anwendung findet. Diese Ausschlussklausel beruht auf einem subjektiven und objektiven Doppelkriterium. So sind vom Anwendungsbereich der Verordnung Datenverarbeitungen erstens durch die „zuständigen Behörden“ und zweitens zu den in dieser Vorschrift aufgeführten Zwecken ausgeschlossen. Daher sind die verschiedenen vom PNR-Gesetz erfassten Arten von Datenverarbeitungen anhand dieses Doppelkriteriums zu prüfen.

42. Was als Erstes Datenverarbeitungen durch (Luft-, Eisenbahn-, Land- und See-) Beförderungsunternehmen oder durch Reiseunternehmen *zur Erbringung von Dienstleistungen oder zu kommerziellen Zwecken* angeht, so werden diese, sofern im PNR-Gesetz genannt, weiterhin durch die DSGVO geregelt, da weder der subjektive noch der objektive Teil des in Art. 2 Abs. 2 Buchst. d dieser Verordnung enthaltenen Ausschlusskriteriums erfüllt ist.

43. Was als Zweites die *Übermittlung von PNR-Daten durch Beförderungsunternehmen oder Reiseunternehmen an die PNR-Zentralstelle* betrifft, die als solche eine „Verarbeitung“ im Sinne von Art. 4 Nr. 2 der DSGVO darstellt [20], so ist ihre Einbeziehung in den Anwendungsbereich dieser Verordnung weniger offensichtlich.

[17] In Art. 2 Abs. 1 der DSGVO heißt es: „Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

[18] Vgl. in diesem Sinne Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504, Rn. 61).

[19] Vgl. Urteil vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, EU:C:2020:559, Rn. 84), sowie Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504, Rn. 62).

[20] Vgl. in diesem Sinne Urteil vom 6. Oktober 2020, Privacy International (C-623/17, im Folgenden: Urteil Privacy International, EU:C:2020:790, Rn. 41 und die dort angeführte Rechtsprechung). Gemäß Art. 4 Nr. 2 der DSGVO stellt „jede[r] … Vorgang … im Zusammenhang mit personenbezogenen Daten wie … die Offenlegung durch Übermittlung“ eine „Verarbeitung“ dar.

44. Zum einen wird diese Übermittlung nämlich nicht von einer „zuständigen Behörde“ im Sinne von Art. 3 Nr. 7 der Polizei-Richtlinie, auf die in Ermangelung einer Definition dieses Begriffs in der DSGVO entsprechend Bezug zu nehmen ist, vorgenommen [21]. Ein Wirtschaftsteilnehmer wie beispielsweise ein Beförderungsunternehmen oder ein Reiseunternehmen, dem lediglich eine Rechtspflicht zur Übermittlung personenbezogener Daten obliegt und keinerlei hoheitliche Befugnisse übertragen worden sind [22], kann nicht als Stelle oder Einrichtung im Sinne von Art. 3 Nr. 7 Buchst. b angesehen werden [23].

45. Zum anderen wird die Übermittlung von PNR-Daten durch Beförderungsunternehmen und Reiseunternehmen vorgenommen, um eine gesetzlich vorgeschriebene Verpflichtung zu erfüllen, mit dem Ziel, die Verfolgung der in Art. 2 Abs. 2 Buchst. d der DSGVO aufgeführten Zwecke zu ermöglichen.

46. Aus dem Wortlaut dieser Vorschrift geht nach meinem Dafürhalten jedoch eindeutig hervor, dass nur Verarbeitungen, die sowohl den subjektiven Teil als auch den objektiven Teil des in ihr genannten Ausschlusskriteriums erfüllen, nicht in den Anwendungsbereich der DSGVO fallen. Die den Beförderungsunternehmen und den Reiseunternehmen durch das PNR-Gesetz auferlegte Verpflichtung zur Übermittlung von PNR-Daten an die PNR-Zentralstelle fällt daher unter diese Verordnung.

47. Hinsichtlich der Bestimmungen des PNR-Gesetzes zur Umsetzung der PNR-Richtlinie wird die vorstehende Schlussfolgerung durch Art. 21 Abs. 2 dieser Richtlinie untermauert, der vorsieht, dass die Richtlinie „nicht die Anwendbarkeit der Richtlinie 95/46/EG[[24]] auf die Verarbeitung personenbezogener Daten durch Fluggesellschaften [berührt]“. Die u. a. von der französischen Regierung vorgeschlagene Auslegung der Vorschrift, wonach diese lediglich vorsehe, dass die Beförderungsunternehmen hinsichtlich der nicht in der PNR-Richtlinie vorgesehenen Datenverarbeitungen weiterhin den in der DSGVO festgelegten Verpflichtungen unterlägen, muss nach meinem Dafürhalten zurückgewiesen werden. In Anbetracht ihres Wortlauts hat diese „Vorbehaltsklausel“ nämlich einen breiten Anwendungsbereich und definiert sich ausschließlich durch einen Verweis auf den Datenverarbeiter, da vom Zweck oder vom Rahmen der Verarbeitung, wenn sie in Ausübung der Geschäftstätigkeit der Fluggesellschaft oder in Durchführung einer rechtlichen Verpflichtung erfolgt, keine Rede ist. Außerdem ist eine inhaltsgleiche Klausel in Art. 13 Abs. 3 der PNR-Richtlinie enthalten, der sich ganz konkret auf die den Fluggesellschaften nach der DSGVO obliegenden Pflichten bezieht, „geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit und Vertraulichkeit der personenbezogenen Daten zu treffen“. Diese Vorschrift gehört jedoch zu den Vorschriften, die

21 Vgl. in diesem Sinne Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504, Rn. 69). Gemäß Art. 3 Nr. 7 Buchst. a und b der Polizei-Richtlinie ist eine „zuständige Behörde“ „a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder b) eine andere Stelle oder Einrichtung, der durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse [zu den gleichen Zwecken] übertragen wurde“.

22 Der Vorlageentscheidung ist kein Anhaltspunkt in diesem Sinne zu entnehmen.

23 Ein solcher Wirtschaftsteilnehmer kann auch nicht als „Auftragsverarbeiter“ im Sinne von Art. 4 Nr. 8 der DSGVO oder Art. 3 Nr. 9 der Polizei-Richtlinie eingestuft werden, da es sich bei ihm eher um einen „Verantwortlichen“ im Sinne von Art. 4 Nr. 7 Satz 2 der DSGVO handelt. Gemäß Art. 4 Nr. 8 der DSGVO und Art. 3 Nr. 9 der Polizei-Richtlinie, die im gleichen Wortlaut abgefasst sind, ist ein „Auftragsverarbeiter“ eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Im Sinne von Art. 4 Nr. 7 Satz 1 der DSGVO ist ein „Verantwortlicher“ „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die … über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, wobei Satz 2 klarstellt, dass, wenn „die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben [sind], … der Verantwortliche beziehungsweise … die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden [kann bzw. können]“.

24 Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31). Diese Richtlinie ist durch die DSGVO aufgehoben und ersetzt worden, vgl. Art. 94 der DSGVO.

den Schutz gemäß der PNR-Richtlinie verarbeiteter personenbezogener Daten regeln, und folgt auf Art. 13 Abs. 1, der Datenverarbeitungen nach der PNR-Richtlinie allgemein den in ihm genannten Bestimmungen des Rahmenbeschlusses 2008/977 unterwirft. Entgegen dem Vorbringen der französischen Regierung lässt sich mit einer solchen normativen Anordnung zum einen Art. 13 Abs. 3 wie eine Klausel lesen, die nur in der PNR-Richtlinie vorgesehene und nicht von „zuständigen Behörden" im Sinne der Polizei-Richtlinie vorgenommene Datenverarbeitungen unter die DSGVO subsumiert, und zum anderen der Verweis auf die Einhaltung der durch diese Verordnung auferlegten Pflichten im Bereich der Sicherheit und Vertraulichkeit der Daten wie ein Hinweis auf die Garantien verstehen, mit denen die Übermittlung der PNR-Daten durch die Beförderungsunternehmen an die PNR-Zentralstellen zwangsläufig versehen sein müssen.

48. Die Schlussfolgerung in Nr. 46 der vorliegenden Schlussanträge wird durch den 19. Erwägungsgrund der DSGVO und den elften Erwägungsgrund der Polizei-Richtlinie, auf die u. a. die deutsche, die irische und die französische Regierung in ihrem Vorbringen verweisen, die PNR-Richtlinie sei eine *lex specialis*, nicht in Frage gestellt. Daran ist zwar richtig, dass mit der PNR-Richtlinie für die in ihr genannten Verarbeitungen personenbezogener Daten ein gegenüber der DSGVO eigenständiger Rahmen zum Datenschutz geschaffen wird. Dieser spezifische Rahmen gilt jedoch nur für Verarbeitungen von PNR-Daten durch „zuständige Behörden" im Sinne von Art. 3 Nr. 7 der Polizei-Richtlinie, zu denen insbesondere die PNR-Zentralstellen gehören, während die Übermittlung von PNR-Daten an die PNR-Zentralstellen in Anwendung u. a. der in Art. 21 Abs. 2 der PNR-Richtlinie vorgesehenen „Vorbehaltsklausel" dem mit der DSGVO geschaffenen allgemeinen Rahmen unterworfen bleibt.

49. Zur Stützung ihrer Auffassung, wonach die DSGVO nicht für die Übermittlung von PNR-Daten durch Beförderungsunternehmen und Reiseunternehmen an die PNR-Zentralstellen gelte, verweisen die belgische, die irische, die französische und die zyprische Regierung auf das Urteil vom 30. Mai 2006, Parlament/Rat und Kommission [25], in dem der Gerichtshof für Recht erkannt hat, dass die Übermittlung von PNR-Daten durch Fluggesellschaften der Gemeinschaft an die Behörden der Vereinigten Staaten von Amerika im Rahmen eines zwischen diesen und der Europäischen Gemeinschaft ausgehandelten Abkommens eine Verarbeitung personenbezogener Daten im Sinne von Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 [26] darstellt und daher nicht in den Anwendungsbereich dieser Richtlinie fällt. Bei seiner Entscheidung hat der Gerichtshof den *Zweck der Übermittlung* sowie die Tatsache berücksichtigt, dass diese „in einem von staatlichen Stellen geschaffenen Rahmen statt[fand]", obwohl die Daten von privaten Wirtschaftsteilnehmern erhoben und übermittelt wurden [27].

[25] C-317/04 und C-318/04, im Folgenden: Urteil Parlament/Rat, EU:C:2006:346. In den Rechtssachen, in denen dieses Urteil ergangen ist, hatte das Parlament zum einen die Nichtigerklärung des Beschlusses 2004/496/EG des Rates vom 17. Mai 2004 über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (ABl. 2004, L 183, S. 83, berichtigt in ABl. 2005, L 255, S. 168) und zum anderen die Nichtigerklärung der Entscheidung 2004/535/EG der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden (ABl. 2004, L 235, S. 11) beantragt.

[26] Gemäß Art. 3 Abs. 2 erster Gedankenstrich der Richtlinie 95/46 fand diese Richtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten, „die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des Vertrags über die Europäische Union, und *auf keinen Fall* auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich" (Hervorhebung nur hier).

[27] Zum „teleologischen" und „kontextbezogenen" Ansatz des Gerichtshofs im Urteil Parlament/Rat vgl. Schlussanträge des Generalanwalts Campos Sánchez-Bordona in den verbundenen Rechtssachen La Quadrature du Net u. a. (C-511/18 und C-512/18, EU:C:2020:6, Nrn. 47 und 62).

50. Insoweit genügt die Feststellung, dass das Urteil Parlament/Rat, wie der Gerichtshof im Urteil vom 6. Oktober 2020, La Quadrature du Net u. a.[28], im Wesentlichen entschieden hat, nicht auf den Kontext der DSGVO übertragbar ist[29].

51. Darüber hinaus hat der Gerichtshof die Argumentation, der er in den Urteilen Tele2 Sverige und vom 2. Oktober 2018, Ministerio Fiscal[30], gefolgt ist, in Rn. 102 des Urteils La Quadrature du Net[31] analog angewandt und festgestellt: „Die [DSGVO] findet zwar nach ihrem Art. 2 Abs. 2 Buchst. d keine Anwendung auf Verarbeitungen ‚durch die zuständigen Behörden' u. a. zum Zweck der Verhütung und Feststellung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Wie aus Art. 23 Abs. 1 Buchst. d und h der Verordnung hervorgeht, fallen aber Verarbeitungen personenbezogener Daten, die zu diesem Zweck von Privatpersonen vorgenommen werden, in ihren Anwendungsbereich."[32]

52. Aus den bereits dargelegten Gründen bin ich davon überzeugt, dass sich die Schlussfolgerung, wonach die Übermittlung von PNR-Daten durch die Beförderungsunternehmen und die Reiseunternehmen an die PNR-Zentralstellen unter die DSGVO fällt, bereits klar aus dem Wortlaut von Art. 2 Abs. 2 Buchst. d der DSGVO ergibt, der sich nur auf Verarbeitungen durch „zuständige Behörden" bezieht, ohne dass es erforderlich ist, auf die in Art. 23 Abs. 1 dieser Verordnung enthaltene Beschränkungsklausel Bezug zu nehmen[33]. Dessen ungeachtet stellt die in Rn. 102 des Urteils La Quadrature du Net enthaltene Feststellung ein klares Bekenntnis des Gerichtshofs zugunsten einer solchen Schlussfolgerung dar.

53. Da die Übermittlung von PNR-Daten durch Beförderungsunternehmen und Reiseunternehmen in den Anwendungsbereich der DSGVO fällt, stellen nationale Rechtsvorschriften wie das PNR-Gesetz, das diese Unternehmen zur Vornahme einer solchen Übermittlung verpflichtet, eine „Gesetzgebungsmaßnahme" gemäß Art. 23 Abs. 1 Buchst. d der DSGVO dar und müssen daher die darin vorgesehenen Voraussetzungen erfüllen[34].

54. Was als Drittes Verarbeitungen von PNR-Daten *durch die PNR-Zentralstelle und die zuständigen nationalen Behörden* angeht, hängt die Anwendbarkeit der DSGVO, wie aus den vorstehenden Ausführungen hervorgeht, von den Zwecken ab, die mit diesen Verarbeitungen verfolgt werden.

55. So sind erstens Verarbeitungen von PNR-Daten durch die PNR-Zentralstelle und die zuständigen nationalen Behörden zu den in Art. 8 § 1 Nrn. 1 bis 3 und 5 des PNR-Gesetzes aufgeführten Zwecken[35] vom Anwendungsbereich der DSGVO ausgeschlossen, soweit diese Zwecke, wie es der Fall zu sein scheint, zu den Zwecken gehören, die von der Ausschlussklausel in Art. 2 Abs. 2 Buchst. d der DSGVO erfasst werden. Der Schutz der Daten der von den

28 C-511/18, C-512/18 und C-520/18, im Folgenden: Urteil La Quadrature du Net, EU:C:2020:791.

29 Vgl. Urteil La Quadrature du Net (Rn. 100 bis 102).

30 C-207/16, im Folgenden: Urteil Ministerio Fiscal, EU:C:2018:788, Rn. 34.

31 Vgl. in diesem Sinne auch Urteil Privacy International (Rn. 47).

32 Vgl. entsprechend Urteile Tele2 Sverige (Rn. 72 bis 74) und Ministerio Fiscal (Rn. 34). Diese Urteile bezogen sich auf die Auslegung von Art. 15 Abs. 1 Satz 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37), der eine Beschränkungsklausel vorsieht, die der in Art. 23 Abs. 1 Buchst. a bis d der DSGVO enthaltenen ähnlich ist.

33 Im Kontext der Richtlinie 2002/58 war eine Bezugnahme auf deren Art. 15 Abs. 1 in Anbetracht des Wortlauts der in Art. 1 Abs. 3 dieser Richtlinie vorgesehenen Ausschlussklausel, die sich allgemein auf „Tätigkeiten des Staates im strafrechtlichen Bereich" bezieht, gerechtfertigt.

34 Vgl. entsprechend Urteil Privacy International (Rn. 38 und 39).

35 Es handelt sich um Verarbeitungen, die durch die Kapitel 7 bis 10 und 12 des PNR-Gesetzes geregelt werden.

Verarbeitungen betroffenen Personen fällt unter das nationale Recht, vorbehaltlich der Anwendung der Polizei-Richtlinie [36] und – im Rahmen ihres Anwendungsbereichs – der PNR-Richtlinie.

56. Gleiches gilt zweitens für Verarbeitungen von PNR-Daten durch die PNR-Zentralstelle und die Sicherheits- und Nachrichtendienste im Rahmen der Beaufsichtigung der in den Bestimmungen des Grundlagengesetzes über die Nachrichten- und Sicherheitsdienste erwähnten Aktivitäten, die in Art. 8 § 1 Nr. 4 des PNR-Gesetzes aufgeführt sind, soweit sie die in Art. 2 Abs. 2 Buchst. d der DSGVO genannten Zwecke erfüllen, was das vorlegende Gericht zu beurteilen hat.

57. Die belgische Regierung trägt vor, Verarbeitungen gemäß Art. 8 § 1 Nr. 4 des PNR-Gesetzes würden in jedem Fall von den Ausschlussklauseln in Art. 2 Abs. 2 Buchst. a der DSGVO und in Art. 2 Abs. 3 Buchst. a der Polizei-Richtlinie erfasst, da die Tätigkeiten der Sicherheits- und Nachrichtendienste nicht in den Anwendungsbereich des Unionsrechts fielen.

58. Obwohl der Gerichtshof nicht zur Auslegung dieser Vorschriften befragt wird, stelle ich insoweit zunächst fest, dass, wie der Gerichtshof bereits entschieden hat, eine nationale Regelung, die privaten Wirtschaftsteilnehmern Verarbeitungspflichten auferlegt, selbst dann unter die Bestimmungen des Unionsrechts im Bereich des Schutzes personenbezogener Daten fällt, wenn sie den Schutz der nationalen Sicherheit betrifft [37]. Folglich fällt die Übermittlung von PNR-Daten, die den Beförderungsunternehmen und den Reiseunternehmen durch das PNR-Gesetz vorgeschrieben wird, grundsätzlich selbst dann unter die DSGVO, wenn sie zu den Zwecken von Art. 8 § 1 Nr. 4 dieses Gesetzes erfolgt.

59. Sodann weise ich darauf hin, dass die DSGVO nach ihrem 16. Erwägungsgrund zwar nicht für „die nationale Sicherheit betreffende Tätigkeiten“ gilt und, wie der 14. Erwägungsgrund der Polizei-Richtlinie klarstellt, „die nationale Sicherheit betreffende Tätigkeiten [und] Tätigkeiten von Agenturen oder Stellen, die mit Fragen der nationalen Sicherheit befasst sind, … nicht als Tätigkeiten betrachtet werden [sollten], die in den Anwendungsbereich dieser Richtlinie fallen“, die Kriterien, auf deren Grundlage eine Verarbeitung personenbezogener Daten durch eine öffentliche Behörde, Stelle oder Agentur eines Mitgliedstaats in den Anwendungsbereich eines der beiden Unionsrechtsakte zur Regelung des Schutzes der betreffenden Personen bei solchen Verarbeitungen fällt oder außerhalb des Anwendungsbereichs des Unionsrechts liegt, aber einer Logik folgen, die sowohl mit den dieser Behörde, Stelle oder Agentur zugewiesenen Funktionen als auch mit den Zwecken der Verarbeitung zusammenhängt. Deshalb hat der Gerichtshof entschieden, dass Art. 2 Abs. 2 Buchst. a der DSGVO im Licht des 16. Erwägungsgrundes dieser Verordnung „so zu verstehen ist, dass damit vom Anwendungsbereich dieser Verordnung allein Verarbeitungen personenbezogener Daten ausgenommen werden sollen, die von staatlichen Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann, vorgenommen werden, so dass der bloße Umstand, dass eine Tätigkeit eine spezifische Tätigkeit des Staates oder einer Behörde ist, nicht dafür ausreicht, dass diese Ausnahme automatisch für diese Tätigkeit gilt“ [38]. Er hat darüber hinaus klargestellt, dass „[d]ie auf die Wahrung der nationalen Sicherheit abzielenden Tätigkeiten, auf die Art. 2 Abs. 2 Buchst. a der DSGVO abstellt, … insbesondere solche [umfassen], die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken“ [39]. Für den Fall, dass ein Mitgliedstaat seinen Sicherheits- und

36 Vgl. in diesem Sinne Urteile La Quadrature du Net (Rn. 103) und Privacy International (Rn. 48).

37 Vgl. u. a. Urteil La Quadrature du Net.

38 Vgl. Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504, Rn. 66).

39 Vgl. Urteil vom 22. Juni 2021, Latvijas Republikas Saeima (Strafpunkte) (C-439/19, EU:C:2021:504).

Nachrichtendiensten Aufgaben in den in Art. 3 Nr. 7 Buchst. a der Polizei-Richtlinie aufgeführten Bereichen überträgt, würden die von den Diensten für die Erfüllung dieser Aufgaben vorgenommenen Datenverarbeitungen folglich in den Anwendungsbereich der Polizei-Richtlinie und gegebenenfalls der PNR-Richtlinie fallen. Ich stelle ganz allgemein fest, dass, wie der Gerichtshof im Rahmen der Auslegung von Art. 4 Abs. 2 EUV, auf den sich u. a. die belgische Regierung stützt, wiederholt entschieden hat, die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen Sicherheit getroffen wurde, nicht zur Unanwendbarkeit des Unionsrechts führen und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbinden kann [40], weshalb sich der Gerichtshof zurückhaltend zeigt, wenn es um einen automatischen und gänzlichen Ausschluss der Tätigkeiten der Mitgliedstaaten im Zusammenhang mit dem Schutz der nationalen Sicherheit vom Anwendungsbereich des Unionsrechts geht.

60. Drittens ist in Übereinstimmung mit allen Verfahrensbeteiligten, die Erklärungen abgegeben haben, mit Ausnahme der französischen Regierung davon auszugehen, dass Verarbeitungen von PNR-Daten durch die zuständigen belgischen Behörden zu den in Art. 8 § 2 des PNR-Gesetzes genannten Zwecken, nämlich „um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen“ [41], weder unter die in Art. 2 Abs. 2 Buchst. d der DSGVO enthaltene Ausschlussklausel noch unter einen anderen in diesem Artikel vorgesehenen Ausschlussgrund und daher in den Anwendungsbereich der Verordnung fallen. Entgegen dem Vorbringen der französischen Regierung unterliegen solche Verarbeitungen weder der PNR-Richtlinie, deren Art. 1 Abs. 2 vorsieht, dass „[d]ie nach Maßgabe dieser Richtlinie erhobenen PNR-Daten … ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität … verarbeitet werden [dürfen]“, noch grundsätzlich der Polizei-Richtlinie, die nach ihrem Art. 1 Abs. 1 nur für Verarbeitungen personenbezogener Daten durch die zuständigen Behörden „zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“, gilt. Wie aus der Vorlageentscheidung hervorgeht, sollen mit Art. 8 § 2 des PNR-Gesetzes und dessen Kapitel 11, das Bestimmungen über die Verarbeitung von PNR-Daten zur Verbesserung der Kontrolle an den Grenzen und zur Bekämpfung der illegalen Einwanderung enthält und dazu die Übermittlung dieser Daten durch die PNR-Zentralstelle u. a. an die mit der Grenzkontrolle beauftragten Polizeidienste vorsieht, die API-Richtlinie und die Richtlinie 2010/65 in belgisches Recht umgesetzt werden. Beide Richtlinien verpflichten die zuständigen Behörden hinsichtlich der in ihnen vorgesehenen Verarbeitungen zur Einhaltung der Bestimmungen der Richtlinie 95/46 [42]. Entgegen dem Vorbringen der französischen Regierung ist der Verweis auf die Schutzbestimmungen dieser Richtlinie so zu verstehen, dass er Verarbeitungen personenbezogener Daten nach der API-Richtlinie und der Richtlinie 2010/65 umfasst. Die Tatsache, dass die API-Richtlinie aus der Zeit vor dem Inkrafttreten des Rahmenbeschlusses 2008/977 stammt, ist insoweit irrelevant, da dieser Rahmenbeschluss und die Polizei-Richtlinie, die ihn ersetzt hat, nur die in Art. 3 Abs. 1 der API-Richtlinie genannten Verarbeitungen personenbezogener Daten durch die zuständigen Behörden zu Strafverfolgungszwecken betreffen [43].

40 Vgl. Urteil La Quadrature du Net (Rn. 99 und die dort angeführte Rechtsprechung).

41 Die Voraussetzungen für diese Datenverarbeitungen sind in Kapitel 11 des PNR-Gesetzes geregelt.

42 Vgl. Erwägungsgründe 8, 9 und 12 sowie Art. 6 der API-Richtlinie und Art. 8 Abs. 2 der Richtlinie 2010/65.

43 Die Verwendung der erweiterten Fluggastdaten (im Folgenden: API-Daten) durch die Strafverfolgungsbehörden ist in Art. 6 Abs. 1 letzter Unterabsatz der API-Richtlinie ausdrücklich vorgesehen.

61. Nach alledem schlage ich dem Gerichtshof vor, auf die erste Vorlagefrage zu antworten, dass Art. 23 der DSGVO in Verbindung mit Art. 2 Abs. 2 Buchst. d dieser Verordnung dahin auszulegen ist, dass er

– für nationale Rechtsvorschriften zur Umsetzung der PNR-Richtlinie gilt, soweit diese Rechtsvorschriften Verarbeitungen von PNR-Daten durch Beförderungsunternehmen und andere Wirtschaftsteilnehmer, einschließlich der in Art. 8 der Richtlinie vorgesehenen Übermittlung von PNR-Daten an die PNR-Zentralstellen, regeln;

– nicht für nationale Rechtsvorschriften zur Umsetzung der PNR-Richtlinie gilt, soweit diese Rechtsvorschriften Datenverarbeitungen durch die zuständigen nationalen Behörden, einschließlich der PNR-Zentralstellen und gegebenenfalls der Sicherheits- und Nachrichtendienste des betreffenden Mitgliedstaats, zu den in Art. 1 Abs. 2 der Richtlinie vorgesehenen Zwecken regeln;

– für nationale Rechtsvorschriften zur Verbesserung der Personenkontrolle an den Außengrenzen und zur Bekämpfung der illegalen Einwanderung gilt, mit denen die API-Richtlinie und die Richtlinie 2010/65 umgesetzt werden.

B. Zur zweiten, zur dritten, zur vierten, zur sechsten und zur achten Vorlagefrage

62. Mit seiner zweiten, seiner dritten, seiner vierten und seiner sechsten Vorlagefrage befragt der Verfassungsgerichtshof den Gerichtshof zur Gültigkeit der PNR-Richtlinie in Bezug auf die Art. 7, 8 und 52 Abs. 1 der Charta. Obwohl sie wie eine Auslegungsfrage abgefasst ist, zielt auch die achte Vorlagefrage im Wesentlichen darauf ab, den Gerichtshof zu veranlassen, sich zur Gültigkeit dieser Richtlinie zu äußern.

63. Mit den Fragen, die sich auf die verschiedenen Elemente des durch die PNR-Richtlinie geschaffenen Systems zur Verarbeitung von PNR-Daten beziehen, wird für jedes einzelne dieser Elemente um Beurteilung der Frage ersucht, ob es die Voraussetzungen erfüllt, von denen die Rechtmäßigkeit der Beschränkungen für die Ausübung der in den Art. 7 und 8 der Charta niedergelegten Grundrechte abhängt. So betreffen die zweite und die dritte Vorlagefrage den Katalog der PNR-Daten in Anhang I, die vierte Frage die Definition des Begriffs „Fluggast“ in Art. 3 Nr. 4 der PNR-Richtlinie, die sechste Frage die Verwendung der PNR-Daten für die Vorabüberprüfung gemäß Art. 6 dieser Richtlinie und die achte Frage die in Art. 12 Abs. 1 der Richtlinie vorgesehene Frist für die Speicherung der PNR-Daten.

1. Zu den in den Art. 7 und 8 der Charta niedergelegten Grundrechten

64. Art. 7 der Charta garantiert jeder Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Kommunikation. Art. 8 Abs. 1 der Charta räumt jeder Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten ein. Nach ständiger Rechtsprechung sind diese Rechte, die sich auf jede Information erstrecken, die eine bestimmte oder bestimmbare natürliche Person betrifft, eng miteinander verknüpft, da der Zugriff auf personenbezogene Daten einer natürlichen Person zum Zweck ihrer Speicherung oder Verwendung das Recht dieser Person auf Achtung des Privatlebens berührt [44].

[44] Vgl. in diesem Sinne u. a. Urteil vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, EU:C:2020:559, Rn. 170 und die dort angeführte Rechtsprechung).

65. Die in den Art. 7 und 8 der Charta niedergelegten Rechte können jedoch keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden [45]. Art. 8 Abs. 2 der Charta gestattet daher die Verarbeitung personenbezogener Daten, wenn bestimmte Voraussetzungen erfüllt sind. Diese Vorschrift sieht vor, dass personenbezogene Daten nur „nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ verarbeitet werden dürfen.

66. Jede Einschränkung des Rechts auf Schutz personenbezogener Daten und des Rechts auf Privatsphäre muss außerdem die Vorgaben von Art. 52 Abs. 1 der Charta beachten. So muss eine solche Einschränkung gesetzlich vorgesehen sein, den Wesensgehalt dieser Rechte achten und unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sein und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

67. Bei der Beurteilung einer die genannten Rechte einschränkenden Maßnahme muss auch berücksichtigt werden, welche Bedeutung den in den Art. 3, 4, 6 und 7 der Charta verankerten Rechten und den Zielen des Schutzes der nationalen Sicherheit und der Bekämpfung schwerer Kriminalität als Beitrag zum Schutz der Rechte und Freiheiten anderer zukommt [46]. Insoweit ist in Art. 6 der Charta das Recht jedes Menschen nicht nur auf Freiheit, sondern auch auf Sicherheit verankert [47].

68. Darüber hinaus soll mit Art. 52 Abs. 3 der Charta die notwendige Kohärenz zwischen den in der Charta enthaltenen Rechten und den entsprechenden durch die EMRK garantierten Rechten, die als Mindestschutzstandard zu berücksichtigen sind, gewährleistet werden [48]. Das in Art. 7 der Charta verankerte Recht auf Achtung des Privat- und Familienlebens entspricht dem in Art. 8 EMRK garantierten Recht, so dass ihm die gleiche Bedeutung und Tragweite zuzuerkennen ist [49]. Aus der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (im Folgenden: EGMR) geht hervor, dass ein Eingriff in die in diesem Artikel garantierten Rechte nach Art. 8 Abs. 2 nur gerechtfertigt sein kann, wenn er gesetzlich vorgesehen ist, einem oder mehreren darin aufgeführten rechtmäßigen Zielen dient und in einer demokratischen Gesellschaft zur Erreichung dieses Ziels oder dieser Ziele erforderlich ist [50]. Die Maßnahme muss auch mit dem Grundsatz der Rechtsstaatlichkeit vereinbar sein, der in der Präambel der EMRK ausdrücklich erwähnt wird und Ziel und Zweck von deren Art. 8 inhärent ist [51].

69. Im Licht der vorstehend aufgeführten Grundsätze sind die Gültigkeitsfragen des Verfassungsgerichtshofs zu prüfen.

45 Vgl. u. a. Urteil vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, EU:C:2020:559, Rn. 172 und die dort angeführte Rechtsprechung).

46 Vgl. in diesem Sinne Urteil La Quadrature du Net (Rn. 122).

47 Vgl. Urteil La Quadrature du Net (Rn. 123).

48 Vgl. Urteil La Quadrature du Net (Rn. 124 und die dort angeführte Rechtsprechung).

49 Vgl. Urteil vom 18. Juni 2020, Kommission/Ungarn (Transparenz von Vereinigungen) (C-78/18, EU:C:2020:476, Rn. 122 und die dort angeführte Rechtsprechung).

50 Vgl. u. a. EGMR, 4. Dezember 2015, Roman Zakharov/Russland (CE:ECHR:2015:1204JUD004714306, § 227); EGMR, 18. Mai 2010, Kennedy/Vereinigtes Königreich (CE:ECHR:2010:0518JUD002683905, § 130), und EGMR, 25. Mai 2021, Centrum för Rättvisa/Schweden (CE:ECHR:2021:0525JUD003525208, § 246).

51 Vgl. EGMR, 4. Dezember 2015, Roman Zakharov/Russland, (CE:ECHR:2015:1204JUD004714306, § 228); EGMR, 4. Mai 2000, Rotaru/Rumänien (CE:ECHR:2000:0504JUD002834195, § 52); EGMR, 4. Dezember 2008, S. und Marper/Vereinigtes Königreich (CE:ECHR:2008:1204JUD003056204, § 95); EGMR, 18. Mai 2021, Kennedy/Vereinigtes Königreich (CE:ECHR:2010:0518JUD002683905, § 151), sowie EGMR, 25. Mai 2021, Centrum för Rättvisa/Schweden (CE:ECHR:2021:0525JUD003525208, § 246).

2. Zum Eingriff in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte

70. Der Gerichtshof hat bereits entschieden, dass Bestimmungen, die die Übermittlung personenbezogener Daten natürlicher Personen an einen Dritten, etwa eine Behörde, vorschreiben oder gestatten, bei fehlender Einwilligung dieser natürlichen Personen unabhängig von der späteren Verwendung der in Rede stehenden Daten als Eingriff in ihr Privatleben und damit – unbeschadet ihrer etwaigen Rechtfertigung – als Einschränkung des durch Art. 7 der Charta garantierten Grundrechts einzustufen sind [52]. Dem ist so, auch wenn keine Umstände vorliegen, aufgrund deren ein solcher Eingriff als „schwer" eingestuft werden kann, und ohne dass es darauf ankommt, ob die betroffenen Informationen über das Privatleben als sensibel anzusehen sind oder die Betroffenen durch diesen Eingriff irgendwelche Nachteile erlitten haben [53]. In gleicher Weise stellt der Zugang der öffentlichen Stellen zu solchen Informationen einen Eingriff in das in Art. 8 der Charta garantierte Grundrecht auf Schutz personenbezogener Daten dar, da es sich dabei um eine Verarbeitung personenbezogener Daten handelt [54]. Auch die Vorratsspeicherung von Daten über das Privatleben einer Person während eines bestimmten Zeitraums stellt als solche einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Rechte dar [55].

71. Der Gerichtshof hat ebenfalls bereits entschieden, dass PNR-Daten wie die in Anhang I aufgezählten Informationen über bestimmte natürliche Personen, und zwar die betroffenen Fluggäste, enthalten und dass daher die verschiedenen Verarbeitungen, die mit den PNR-Daten vorgenommen werden können, das Grundrecht auf Achtung des Privatlebens, das in Art. 7 der Charta garantiert ist, berühren. Diese Verarbeitungen fallen zudem unter Art. 8 der Charta und müssen deshalb zwangsläufig die dort vorgesehenen Erfordernisse des Datenschutzes erfüllen [56].

72. Daher stellen nach der PNR-Richtlinie zulässige Verarbeitungen von PNR-Daten, insbesondere – was für die Zwecke der vorliegenden Rechtssache von Interesse ist – die Übermittlung dieser Daten durch die Fluggesellschaften an die PNR-Zentralstellen, ihre Verwendung durch die PNR-Zentralstellen, ihre spätere Übermittlung an zuständige nationale Behörden im Sinne von Art. 7 der PNR-Richtlinie und ihre Aufbewahrung, lauter Eingriffe in die durch die Art. 7 und 8 der Charta garantierten Grundrechte dar.

73. Zur Schwere dieser Eingriffe ist erstens zu bemerken, dass die PNR-Richtlinie eine *systematische* und *kontinuierliche* Übermittlung der PNR-Daten aller Fluggäste im Sinne von Art. 3 Nr. 4 dieser Richtlinie auf einem „Drittstaatsflug" im Sinne von deren Art. 3 Nr. 2 an die PNR-Zentralstellen vorsieht. Eine solche Übermittlung impliziert einen allgemeinen Zugang der PNR-Zentralstellen zu allen gemeldeten PNR-Daten [57]. Diese Feststellung wird entgegen dem von einigen Mitgliedstaaten im vorliegenden Verfahren angeführten Vorbringen nicht durch den Umstand in Frage gestellt, dass die Daten einer automatisierten Verarbeitung unterliegen und die PNR-Zentralstellen deshalb konkret nur zu den Daten Zugang haben werden, deren Auswertung

52 Vgl. u. a. Urteil vom 18. Juni 2020, Kommission/Ungarn (C-78/18, EU:C:2020:476, Rn. 124 und 126 sowie die dort angeführte Rechtsprechung); vgl. auch EGMR, 4. Mai 2000, Rotaru/Rumänien (CE:ECHR:2000:0504JUD002834195, § 48); EGMR, 26. März 1987, Leander/Schweden (CE:ECHR:1987:0326JUD000924881, § 46), sowie EGMR, 29. Juni 2006, Weber und Saravia/Deutschland (CE:ECHR:2006:0629DEC005493400, § 79).

53 Vgl. u. a. Urteil Ministerio Fiscal (Rn. 51 und die dort angeführte Rechtsprechung).

54 Vgl. u. a. Urteile vom 18. Juni 2020, Kommission/Ungarn (C-78/18, EU:C:2020:476, Rn. 126), und Ministerio Fiscal (Rn. 51 und die dort angeführte Rechtsprechung).

55 Vgl. Urteil vom 8. April 2014, Digital Rights Ireland u. a. (C-293/12 und C-594/12, im Folgenden: Urteil Digital Rights, EU:C:2014:238, Rn. 34).

56 Vgl. Gutachten 1/15 (Rn. 121 bis 123).

57 Vgl. entsprechend Urteil Privacy International (Rn. 79 und 80 sowie die dort angeführte Rechtsprechung).

zu einem positiven Ergebnis geführt hat. Zum einen hat ein solcher Umstand den Gerichtshof bisher nämlich nicht daran gehindert, im Rahmen ähnlicher Systeme zur automatisierten Verarbeitung „lose“ gesammelter oder auf Vorrat gespeicherter personenbezogener Daten den allgemeinen Charakter des Zugangs der betreffenden öffentlichen Stellen zu solchen Daten zu bejahen. Zum anderen bringt die bloße Weiterleitung personenbezogener Daten an öffentliche Stellen zur Verarbeitung und Aufbewahrung durch diese Stellen von vornherein deren allgemeinen und vollständigen Zugang zu solchen Daten und einen Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten mit sich.

74. Zweitens können die Mitgliedstaaten gemäß Art. 2 Abs. 1 der PNR-Richtlinie entscheiden, diese auf „EU-Flüge“ im Sinne von deren Art. 3 Nr. 3 anzuwenden. Ich stelle insoweit zum einen fest, dass die PNR-Richtlinie nicht lediglich die Befugnis der Mitgliedstaaten vorsieht, sie auf EU-Flüge auszuweiten, sondern auch die formellen und materiellen Voraussetzungen für die Ausübung dieser Befugnis festlegt [58] und klarstellt, dass, wenn die Befugnis nur für ausgewählte EU-Flüge ausgeübt wird, die Auswahl der Flüge unter Berücksichtigung der mit der Richtlinie verfolgten Ziele zu erfolgen hat [59]. Zum anderen legt die PNR-Richtlinie fest, welche Folgen die Ausübung einer solchen Befugnis hat, indem sie in ihrem Art. 2 Abs. 2 vorsieht, dass, wenn ein Mitgliedstaat beschließt, diese Richtlinie auf EU-Flüge anzuwenden, alle Richtlinienbestimmungen „für EU-Flüge so [gelten], als handele es sich um Drittstaatsflüge, und für PNR-Daten zu EU-Flügen so, als handele es sich um PNR-Daten zu Drittstaatsflügen“.

75. Unter diesen Umständen bin ich entgegen dem Vorbringen mancher Regierungen, die im vorliegenden Verfahren Erklärungen abgegeben haben, der Ansicht, dass die PNR-Richtlinie, obwohl ihre Anwendung auf EU-Flüge von einer Entscheidung der Mitgliedstaaten abhängt, die Rechtsgrundlage für Eingriffe in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten im Zusammenhang mit der Übermittlung, Verarbeitung und Aufbewahrung der PNR-Daten zu diesen Flügen bildet, wenn eine solche Entscheidung getroffen wird.

76. Abgesehen vom Königreich Dänemark, das der PNR-Richtlinie nicht unterliegt [60], wenden fast alle Mitgliedstaaten das mit ihr geschaffene System auf „EU-Flüge“ an [61]. Folglich gilt dieses System für alle Flüge in die Union und aus der Union sowie für nahezu alle Flüge innerhalb der Union.

58 Vgl. Art. 2 Abs. 1 bis 3 der PNR-Richtlinie.

59 Vgl. Art. 2 Abs. 3 der PNR-Richtlinie.

60 Gemäß den Art. 1 und 2 des Protokolls (Nr. 22) über die Position Dänemarks ist dieser Mitgliedstaat, da er sich nicht an der Annahme der PNR-Richtlinie beteiligt, weder durch diese gebunden noch zu ihrer Anwendung verpflichtet (vgl. 40. Erwägungsgrund der PNR-Richtlinie). Aus den von der dänischen Regierung eingereichten schriftlichen Erklärungen geht gleichwohl hervor, dass das Königreich Dänemark 2018 ein Gesetz über die Erhebung, Verwendung und Aufbewahrung von PNR-Daten erlassen hat, dessen Bestimmungen weitgehend mit denen der PNR-Richtlinie übereinstimmen. In Bezug auf Irland geht aus dem 39. Erwägungsgrund der PNR-Richtlinie hervor, dass dieser Mitgliedstaat gemäß Art. 3 des Protokolls (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts, das dem EUV und dem AEUV beigefügt ist, mitgeteilt hat, dass er sich an der Annahme und Anwendung dieser Richtlinie beteiligen möchte.

61 Die Kommission hat eine aktualisierte Liste der Mitgliedstaaten veröffentlicht, die die Anwendung der PNR-Richtlinie auf Flüge innerhalb der EU beschlossen haben – vgl. Art. 2 der [PNR-]Richtlinie (ABl. 2020, C 358, S. 7), berichtigt im September 2021 durch Hinzufügung Sloweniens und Streichung des Verweises auf das Vereinigte Königreich (ABl. 2021, C 360, S. 8). Irland und Österreich stehen nicht auf dieser Liste. Im Bericht der Kommission an das Europäische Parlament und den Rat über die Überprüfung der [PNR-]Richtlinie vom 24. Juli 2020 (KOM[2020] 305 endg., S. 11 [im Folgenden: Bericht der Kommission von 2020]) heißt es, dass alle Mitgliedstaaten außer einem die Erhebung von PNR-Daten auf Flüge innerhalb der EU ausgeweitet haben.

77. Drittens sind, was die zu übermittelnden PNR-Daten angeht, in Anhang I 19 Rubriken aufgeführt, die sich auf biografische Angaben [62], Einzelheiten der Flugreise [63] und weitere im Kontext des Flugbeförderungsvertrags erhobene Daten wie beispielsweise Telefonnummer, E-Mail-Adresse, Zahlungsinformationen, Reisebüro bzw. Sachbearbeiter, Gepäckangaben und allgemeine Hinweise [64] beziehen. Wie der Gerichtshof in Rn. 128 des Gutachtens 1/15 zu den Rubriken im Anhang des Entwurfs eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (im Folgenden: Entwurf eines PNR-Abkommens Kanada–EU), die weitgehend analog zu denen von Anhang I formuliert sind, ausgeführt hat, „können die PNR-Daten, auch wenn einige von ihnen für sich genommen nicht geeignet sein dürften, bedeutsame Informationen über das Privatleben der betreffenden Personen zu liefern, zusammen betrachtet u. a. einen gesamten Reiseverlauf, Reisegewohnheiten, Beziehungen zwischen zwei oder mehreren Personen sowie Informationen über die finanzielle Situation der Fluggäste, ihre Ernährungsgewohnheiten oder ihren Gesundheitszustand offenbaren und sogar sensible Daten über die Fluggäste … liefern“.

78. Viertens sind die von Fluggesellschaften übermittelten Daten gemäß Art. 6 der PNR-Richtlinie dazu bestimmt, von den PNR-Zentralstellen durch automatisierte Verfahren analysiert zu werden, und zwar *systematisch*, d. h. unabhängig von der Frage, ob es den geringsten Hinweis darauf gibt, dass die betreffenden Personen möglicherweise an terroristischen Straftaten oder schwerer Kriminalität beteiligt sind. Insbesondere können die Daten im Rahmen der in Art. 6 Abs. 2 Buchst. a dieser Richtlinie vorgesehenen Vorabüberprüfung von Fluggästen gemäß Abs. 3 durch Abgleich mit „maßgeblichen“ Datenbanken überprüft (Art. 6 Abs. 3 Buchst. a) und anhand im Voraus festgelegter Kriterien abgeglichen (Art. 6 Abs. 3 Buchst. b) werden. Durch die erste Art der Verarbeitung können weitere Informationen über das Privatleben der betreffenden Fluggäste erlangt werden [65]; je nach den für den Abgleich verwendeten Datenbanken kann damit sogar ein *klares Profil* dieser Personen erstellt werden. Daher spiegelt der von mehreren Regierungen erhobene Einwand, wonach die PNR-Richtlinie lediglich Zugang zu einem vergleichsweise kleinen Bestand personenbezogener Daten gestatte, das potenzielle Ausmaß der mit dieser Richtlinie verbundenen Eingriffe in die durch die Art. 7 und 8 der Charta geschützten Grundrechte unter dem Gesichtspunkt des Umfangs der Daten, zu denen sie den Zugang gestatten könnte, nicht angemessen wider. Bezüglich der in Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie vorgesehenen zweiten Art der Datenverarbeitung sei darauf hingewiesen, dass jeder auf im Voraus festgelegten Kriterien beruhende Analysetyp, wie der Gerichtshof in den Rn. 169 und 172 des Gutachtens 1/15 hervorgehoben hat, eine gewisse Fehlerquote, insbesondere eine Reihe „falsch positiver“ Ergebnisse, aufweist. Laut dem Zahlenmaterial im Arbeitspapier der Kommissionsdienststellen [66] (im Folgenden: Arbeitspapier von 2020), das dem Bericht der Kommission von 2020 als Anhang beigefügt ist, ist die Zahl der Treffer, die sich bei der in Art. 6 Abs. 5 der PNR-Richtlinie vorgesehenen individuellen Überprüfung als falsch erwiesen hat, erheblich und belief sich während der Jahre 2018 und 2019 auf wenigstens fünf von sechs identifizierten Personen [67].

62 Vgl. insbesondere Anhang I Nrn. 4 und 18 zu Namen, Geschlecht, Geburtsdatum, Staatsangehörigkeit und Identitätsdokumenten des Fluggasts.

63 Vgl. insbesondere Anhang I Nrn. 2, 3, 7, 13 und 18 der PNR-Richtlinie, in denen u. a. die Flugnummer, die Flughäfen des Abflugs und der Ankunft sowie die Tage und Uhrzeiten des Abflugs und der Ankunft erwähnt werden.

64 Vgl. Anhang I Nrn. 5, 6, 9, 12 und 16.

65 Vgl. in diesem Sinne Gutachten 1/15 (Rn. 131).

66 SWD(2020) 128 endg.

67 Im Arbeitspapier von 2020 (S. 28 und Fn. 55) wird für das Jahr 2019 eine Trefferquote von 0,59 % angegeben, von denen lediglich 0,11 % an die zuständigen Behörden übermittelt worden sind. Für das Jahr 2018 betrugen die entsprechenden Prozentsätze 0,25 % bzw. 0,04 %.

79. Fünftens werden die PNR-Daten gemäß Art. 12 Abs. 1 der PNR-Richtlinie für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen bzw. von dem er abgegangen ist, in einer bei dieser PNR-Zentralstelle angesiedelten Datenbank vorgehalten. Die PNR-Richtlinie ermöglicht es daher, während eines besonders langen Zeitraums über Informationen über das Privatleben der Fluggäste zu verfügen [68]. Da die Übermittlung von PNR-Daten nahezu sämtliche Flüge aus der Union und in die Union sowie innerhalb der Union betrifft und das Flugzeug ein eher gebräuchliches Transportmittel geworden ist, könnten die personenbezogenen Daten eines bedeutenden Teils der Fluggäste darüber hinaus praktisch dauerhaft vorgehalten werden, und zwar schon dann, wenn sie sich wenigstens zwei Mal alle fünf Jahre mit dem Flugzeug fortbewegen.

80. Schließlich sieht die PNR-Richtlinie in allgemeinerer Hinsicht Maßnahmen vor, mit denen zusammen betrachtet auf Unionsebene ein Überwachungssystem geschaffen werden soll, das „nicht zielgerichtet", d. h. nicht durch einen auf einer bestimmten Person oder mehreren bestimmten Personen lastenden Verdacht ausgelöst, „massiv", da es sich auf die personenbezogenen Daten einer großen Zahl von Individuen auswirkt [69], die eine Personengruppe in ihrer Gesamtheit abdecken [70], und „proaktiv" ist, da mit ihm nicht nur bekannte Bedrohungen untersucht, sondern auch bislang unbekannte Gefahren erkannt oder identifiziert werden sollen [71]. Solche Maßnahmen führen naturgemäß zu schweren Eingriffen in die durch die Art. 7 und 8 der Charta geschützten Grundrechte [72], was u. a. mit ihrem präventiven und prädiktiven Zweck zusammenhängt, der eine Auswertung personenbezogener Daten zu breiten Bevölkerungssegmenten erfordert, wobei das Ziel darin besteht, Personen zu „identifizieren", die je nach Ergebnis dieser Auswertung einer eingehenderen Prüfung durch die zuständigen Behörden unterzogen werden sollten [73]. Darüber hinaus haben der vermehrte Rückgriff auf die Verarbeitung großer, „lose" gesammelter Mengen personenbezogener Daten unterschiedlichster Natur sowie ihre Verknüpfung und kombinierte Verarbeitung eine „kumulative Wirkung", die die Einschränkungen der Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten verstärkt und Gefahr läuft, einen Prozess des schrittweisen Übergangs in eine „Überwachungsgesellschaft" zu fördern [74].

68 Vgl. Gutachten 1/15 (Rn. 132).

69 Das mit der PNR-Richtlinie geschaffene System konnte vor der Gesundheitskrise bis zu einer Milliarde einzelne Fluggäste umfassen, Daten zugänglich auf https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table? lang=de.

70 Nämlich jede Person, die dem in Art. 3 Nr. 4 der PNR-Richtlinie definierten Begriff „Fluggast" entspricht und einen „Drittstaatsflug" sowie – *de facto* – einen „EU-Flug" nutzt.

71 In einer von der Europäischen Kommission für Demokratie durch das Recht (Venedig-Kommission) im Jahr 2015 angenommenen Studie wird davon ausgegangen, dass solche Maßnahmen unter den Begriff „strategische Überwachung" fallen und einer „allgemeinen Tendenz" zum Rückgriff auf eine „proaktive Überwachung" der Bevölkerung folgen; vgl. Studie *Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique* (Aktualisierung des Berichts von 2007 über die demokratische Kontrolle der Sicherheitsdienste und Bericht über die demokratische Kontrolle der Agenturen für die Gewinnung von Informationen elektromagnetischen Ursprungs), angenommen von der Venedig-Kommission auf ihrer 102. Plenartagung (Venedig, 20. und 21. März 2015), https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f, Rn. 61.

72 Vgl. – zu Art. 8 EMRK – Urteil des EGMR, 25. Mai 2021, Big Brother Watch u. a./Vereinigtes Königreich (CE:ECHR:2021:0525JUD005817013, § 325, im Folgenden: Urteil Big Brother Watch), über Massenabhörmaßnahmen, in dem der EGMR festgestellt hat, dass die Intensität des Eingriffs in die Ausübung des Rechts auf Achtung des Privatlebens durch diese Maßnahmen mit dem Erreichen der verschiedenen Stufen des Prozesses, nämlich dem Abhören und dem anfänglichen Zurückhalten der Kommunikation und der dazugehörigen Daten, der automatisierten Verarbeitung durch die Anwendung von Selektoren, der Prüfung durch Analysten und dem nachfolgenden Zurückhalten der Daten sowie der Verwendung des „Endprodukts", steigt.

73 Vgl. in diesem Sinne Erwägungsgründe 6 und 7 der PNR-Richtlinie; vgl. für eine eingehende Analyse des Zwecks und der Auswirkungen auf den Schutz des Privatlebens und der personenbezogenen Daten Bericht mit dem Titel *Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards* von Korff, D., unter Mitwirkung von Georges, M., https://rm.coe.int/16806a601b (im Folgenden: Korff-Bericht).

74 Im Korff-Bericht heißt es: „PNR is not an isolated issue, but a new symptom of a much wider disease".

81. Nach alledem muss der mit der PNR-Richtlinie verbundene Eingriff in die durch die Art. 7 und 8 der Charta geschützten Grundrechte meiner Ansicht nach zumindest als „schwer“ eingestuft werden.

82. Zwar könnte, wie insbesondere die Kommission vorträgt, die Gesamtheit der Garantien und Schutzvorkehrungen, die in der PNR-Richtlinie vorgesehen ist, um insbesondere eine missbräuchliche Verwendung der PNR-Daten zu verhindern, die Intensität oder Schwere dieser Eingriffe verringern. Gleichwohl weist jedes System, das den Zugang zu personenbezogenen Daten und deren Verarbeitung durch öffentliche Stellen vorsieht, unter dem Blickwinkel des Schutzes der in Mitleidenschaft gezogenen Grundrechte bereits aufgrund seiner objektiven Merkmale einen gewissen Schweregrad auf. Diesen Schweregrad gilt es nach meinem Dafürhalten zu bestimmen, bevor im Rahmen der Prüfung der Verhältnismäßigkeit der Eingriffe bewertet wird, ob die systemseitig vorgesehenen Garantien hinreichend und angemessen sind. Meines Erachtens ist der Gerichtshof bisher jedenfalls so vorgegangen.

83. Um mit der Charta vereinbar zu sein, müssen die mit der PNR-Richtlinie verbundenen Eingriffe in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten die Voraussetzungen erfüllen, die in den Nrn. 65 und 66 der vorliegenden Schlussanträge aufgeführt sind, was innerhalb der vom vorlegenden Gericht gezogenen Grenzen im Folgenden untersucht werden soll.

3. Zur Rechtfertigung des sich aus der PNR-Richtlinie ergebenden Eingriffs

84. Während sich die dritte Vorlagefrage auf die Einhaltung der in Art. 52 Abs. 1 Satz 1 der Charta genannten Voraussetzung bezieht, wonach jeder Eingriff in ein Grundrecht „gesetzlich vorgesehen“ sein muss, wird der Gerichtshof mit der zweiten, der vierten, der sechsten und der achten Vorlagefrage u. a. zur Einhaltung des Grundsatzes der Verhältnismäßigkeit befragt, auf den Satz 2 dieser Vorschrift abstellt.

a) Zur Einhaltung des Erfordernisses, wonach jede Einschränkung der Ausübung eines in der Charta vorgesehenen Grundrechts gesetzlich vorgesehen sein muss

85. Nach gefestigter Rechtsprechung des Gerichtshofs[75], die sich an der Rechtsprechung des EGMR[76] orientiert, zielt das Erfordernis, wonach jede Einschränkung der Ausübung eines Grundrechts „gesetzlich vorgesehen“ sein muss, nicht nur auf die „rechtliche“ Herkunft des Eingriffs – die in der vorliegenden Rechtssache nicht in Rede steht – ab, sondern bedeutet auch, dass die Rechtsgrundlage für diesen Eingriff dessen Tragweite selbst *klar* und *präzise* festlegen muss. Da sich der zweite Teil des Ausdrucks „gesetzlich vorgesehen“ im Sinne von sowohl Art. 52 Abs. 1 der Charta als auch deren Art. 8 Abs. 2 und Art. 8 EMRK auf die „Qualität des Gesetzes“ und damit auf die Zugänglichkeit und Vorhersehbarkeit der fraglichen Maßnahme bezieht[77], soll er nicht nur die Wahrung des Legalitätsgrundsatzes und einen angemessenen

75 Vgl. u. a. Urteile vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, EU:C:2020:559, Rn. 175), vom 8. September 2020, Recorded Artists Actors Performers (C-265/19, EU:C:2020:677, Rn. 86 und die dort angeführte Rechtsprechung), sowie Privacy international (Rn. 65).

76 Vgl. u. a. Urteile des EGMR vom 8. Juni 2006, Lupsa/Rumänien, (CE:ECHR:2006:0608JUD001033704, §§ 32 und 33), und vom 15. Dezember 2020, Pişkìn/Türkei (CE:ECHR:2020:1215JUD003339918, § 206); vgl. auch Urteil Big Brother Watch (§ 333). Zur Notwendigkeit, dem Ausdruck „gesetzlich vorgesehen“ in Art. 52 Abs. 1 der Charta die gleiche Auslegung zuteilwerden zu lassen, die der EGMR gewählt hat, vgl. Schlussanträge des Generalanwalts Wathelet in der Rechtssache WebMindLicenses (C-419/14, EU:C:2015:606, Nrn. 134 bis 143).

77 Vgl. zuletzt Urteil Big Brother Watch (§ 333).

Schutz gegen Willkür gewährleisten[78], sondern genügt ebenfalls einem Gebot der Rechtssicherheit. Dieses Erfordernis wird auch in der Stellungnahme des Beratenden Ausschusses des Übereinkommens Nr. 108[79] vom 19. August 2016 zu den Auswirkungen der Verarbeitung von Passagierdaten im Bereich des Datenschutzes (im Folgenden: Stellungnahme vom 19. August 2016)[80] aufgestellt.

86. Mit der Annahme der PNR-Richtlinie hat der Unionsgesetzgeber die in den Art. 7 und 8 der Charta niedergelegten Rechte selbst eingeschränkt. Daher können die nach der Richtlinie zulässigen Eingriffe in diese Rechte trotz des Ermessensspielraums, über den die Mitgliedstaaten zum Zeitpunkt ihrer Umsetzung in nationales Recht verfügten, nicht als Folge einer Entscheidung der Mitgliedstaaten angesehen werden[81], sondern finden ihre Rechtsgrundlage in der PNR-Richtlinie selbst. Unter diesen Umständen hatte der Unionsgesetzgeber, um der in Nr. 85 der vorliegenden Schlussanträge in Erinnerung gerufenen Rechtsprechung sowie den „hohen Schutzstandards" für Grundrechte insbesondere in der Charta und in der EMRK, auf die sich der 15. Erwägungsgrund der PNR-Richtlinie bezieht, zu entsprechen, klare und präzise Regeln aufzustellen, aus denen sich sowohl die Tragweite als auch die Anwendung der Maßnahmen, die die Eingriffe beinhalten, ergeben.

87. Mit seiner dritten Vorlagefrage fragt das vorlegende Gericht zwar speziell nach der Einhaltung der Verpflichtung in Bezug auf Anhang I Nrn. 12 und 18; bei der Prüfung der zweiten, der vierten und der sechsten Vorlagefrage, mit denen dieses Gericht an der Erforderlichkeit der mit der PNR-Richtlinie verbundenen Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte zweifelt, wird aber auch zu der Frage Stellung genommen werden müssen, ob die beanstandeten Bestimmungen der PNR-Richtlinie hinreichend klar und präzise sind.

88. Obwohl sich diese Würdigung, wie ich in Nr. 85 der vorliegenden Schlussanträge dargelegt habe, auf die Rechtmäßigkeit des Eingriffs im Sinne von Art. 52 Abs. 1 Satz 1 der Charta bezieht, werde ich darauf – entsprechend dem Ansatz, dem sowohl der Gerichtshof als auch der EGMR in Rechtssachen folgt, in denen es um Maßnahmen geht, die die Verarbeitung personenbezogener Daten zum Gegenstand haben – erst im Rahmen der Prüfung der Verhältnismäßigkeit des Eingriffs eingehen, auf die Satz 2 abstellt[82].

78 Vgl. Urteil vom 17. Dezember 2015, WebMindLicenses (C-419/14, EU:C:2015:832, Rn. 81); vgl. auch EGMR, 1. Juli 2008, Liberty u. a./Vereinigtes Königreich (CE:ECHR:2008:0701JUD005824300, § 69), sowie Urteil Big Brother Watch (§ 333).

79 Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, angenommen in Straßburg am 28. Januar 1981 und ratifiziert von allen Mitgliedstaaten, besser bekannt als „Übereinkommen Nr. 108". Im Jahr 2018 ist ein Protokoll zur Änderung dieses Übereinkommens ausgearbeitet worden, um zu modernisieren. Mit Beschluss (EU) 2019/682 des Rates vom 9. April 2019 (ABl. 2019, L 115, S. 7) sind die Mitgliedstaaten ermächtigt worden, das Änderungsprotokoll im Interesse der Union zu ratifizieren, soweit dessen Bestimmungen in die ausschließliche Zuständigkeit der Union fallen. Im weiteren Verlauf der vorliegenden Schlussanträge werde ich mich auch auf den Text des modernisierten Übereinkommens Nr. 108 beziehen, das, obwohl noch nicht von allen Mitgliedstaaten ratifiziert und noch nicht in Kraft getreten, ausweislich des Beschlusses 2019/682 Schutzbestimmungen enthält, die auf denselben Grundsätzen beruhen wie die in der DSGVO und in der Polizei-Richtlinie genannten.

80 https://rm.coe.int/t-pd-2016-18rev-avis-pnr-fr/16807b6c09, S. 3 und 5. Auch der Erläuternde Bericht zum Protokoll zur Änderung des Übereinkommens Nr. 108 (im Folgenden: Erläuternder Bericht zum modernisierten Übereinkommen Nr. 108) legt den Schwerpunkt auf das Erfordernis, dass die Maßnahme, die Eingriffe in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten vorsieht, „zugänglich", „vorhersehbar", „hinreichend detailliert" und „klar formuliert" sein muss; vgl. Rn. 91 dieses Erläuternden Berichts, https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

81 Vgl. – im Umkehrschluss – Urteil vom 3. Dezember 2019, Tschechische Republik/Parlament und Rat (C-482/17, EU:C:2019:1035, Rn. 135).

82 Vgl. u. a. Urteil La Quadrature du Net (Rn. 132 und die dort angeführte Rechtsprechung); vgl. auch EGMR, Urteil Big Brother Watch (§ 334).

b) Zur Achtung des Wesensgehalts der in den Art. 7 und 8 der Charta niedergelegten Rechte

89. Gemäß Art. 52 Abs. 1 Satz 1 der Charta muss jede Einschränkung der Ausübung der Grundrechte nicht nur auf einer hinreichend genauen Rechtsgrundlage beruhen, sondern auch den *Wesensgehalt* dieser Rechte achten.

90. Wie ich in Nr. 66 der vorliegenden Schlussanträge dargelegt habe, ist dieses Erfordernis – das sich in den Verfassungen verschiedener Mitgliedstaaten wiederfindet [83] und das, obwohl es vom EGMR nicht ausdrücklich anerkannt wird, in dessen Rechtsprechung gleichwohl gut verankert ist [84] – in Art. 52 Abs. 1 der Charta enthalten [85]. Nachdem der Gerichtshof ein solches Erfordernis bereits vor dessen Kodifizierung anerkannt hatte [86], ist es in der Rechtsprechung der Gerichte der Union auch nach Inkrafttreten des Vertrags von Lissabon immer wieder bekräftigt worden.

91. Insbesondere aus dem Urteil vom 6. Oktober 2015, Schrems [87], geht hervor, dass die Verletzung des Wesensgehalts eines Grundrechts durch einen Unionsrechtsakt *automatisch* dessen Nichtigkeit oder Ungültigkeit nach sich zieht, ohne dass es erforderlich ist, eine Abwägung der auf dem Spiel stehenden Interessen vorzunehmen. Der Gerichtshof erkennt daher an, dass jedes Grundrecht einen „harten Kern" hat, der dem Einzelnen einen Freiheitsbereich frei von staatlichen Eingriffen garantiert und der nicht eingeschränkt werden kann [88], ohne das Demokratieprinzip sowie die Grundsätze der Rechtsstaatlichkeit und der Achtung der Menschenwürde, die dem Grundrechtsschutz zugrunde liegen, in Frage zu stellen. Sowohl aus dem Wortlaut von Art. 52 Abs. 1 der Charta als auch aus der Rechtsprechung des Gerichtshofs, insbesondere dem Urteil Schrems I, ergibt sich ferner, dass die Beurteilung der Frage, ob ein Eingriff in den Wesensgehalt des in Rede stehenden Grundrechts vorliegt, vor der Bewertung der Verhältnismäßigkeit der beanstandeten Maßnahme und unabhängig von dieser vorgenommen werden muss. Es handelt sich mit anderen Worten um eine eigenständige Prüfung.

92. Allerdings ist die Bestimmung dessen, was der „Wesensgehalt" eines Grundrechts, das in seiner Ausübung eingeschränkt werden könnte, und daher unantastbar ist, ein äußerst komplexer Vorgang. Auch wenn dieser Begriff, um seine Funktion zu erfüllen, in Anbetracht der wesentlichen Merkmale des in Rede stehenden Grundrechts, der subjektiven und objektiven Ziele, die er schützen will, und ganz allgemein seiner Funktion in einer demokratischen Gesellschaft, die sich auf die Achtung der Menschenwürde gründet, absolut definiert werden können sollte [89], erweist sich ein solcher Vorgang in der Praxis als nahezu unmöglich, zumindest ohne Kriterien, die üblicherweise bei der Prüfung der Verhältnismäßigkeit des Eingriffs in das fragliche Recht herangezogen werden, wie beispielsweise die Schwere dieses Eingriffs, sein Ausmaß oder seine zeitliche Dimension, zu berücksichtigen, ohne also den Besonderheiten des Einzelfalls Rechnung zu tragen.

83 Vgl. insoweit Tridimas, T., Gentile, G. „The essence of Rights: an unreliable Boundary?", *German Law Journal*, 2019, S. 796; Lenaerts, K., „Limits on limitations: The Essence of Fundamental Rights in the EU", *German Law Journal*, 2019, 20, S. 779 f.

84 Seit dem Urteil des EGMR vom 24. Oktober 1979, Winterwerp/Niederlande, (CE:ECHR:1979:1024JUD000630173, § 60).

85 Vgl. Erläuterungen zur Charta der Grundrechte (ABl. 2007, C 303, S. 17, insbesondere „Erläuterung zu Artikel 52", S. 32, im Folgenden: Erläuterungen zur Charta).

86 Vgl. bereits in diesem Sinne u. a. Urteile vom 14. Mai 1974, Nold/Kommission (4/73, EU:C:1974:51, Rn. 14), und vom 13. Dezember 1979, Hauer (44/79, EU:C:1979:290, Rn. 23).

87 C-362/14, im Folgenden: Urteil Schrems I, EU:C:2015:650, Rn. 94 bis 98.

88 Vgl. Lenaerts, K., a. a. O., S. 781; Tridimas, T., Gentile, G., a. a. O., S. 803.

89 In den Erläuterungen zur Charta wird ausdrücklich anerkannt, dass „die Würde des Menschen zum Wesensgehalt der in [der] Charta festgelegten Rechte gehört" und „[s]ie … daher auch bei Einschränkungen eines Rechtes nicht angetastet werden [darf]".

93. Was insbesondere das Grundrecht auf Achtung des Privatlebens angeht, so ist nicht nur zu berücksichtigen, welche Bedeutung es für die geistige und körperliche Gesundheit jedes Menschen, sein Wohlbefinden, seine Autonomie, seine persönliche Entfaltung, seine Fähigkeit, soziale Beziehungen aufzubauen und zu pflegen, sowie dafür hat, dass er über eine Privatsphäre verfügt, in der er seine persönliche Innerlichkeit entwickeln kann, sondern auch, welche Rolle dieses Recht für den Schutz anderer Rechte und Freiheiten wie insbesondere der Gedanken-, der Gewissens-, der Religions-, der Ausdrucks- und der Informationsfreiheit, deren uneingeschränkter Genuss die Wahrung einer Intimsphäre voraussetzt, spielt. Ganz allgemein ist der Funktion Rechnung zu tragen, die die Achtung des Rechts auf Privatleben in einer demokratischen Gesellschaft erfüllt [90]. Der Gerichtshof scheint das Vorliegen einer Beeinträchtigung des Wesensgehalts dieses Rechts zu prüfen, indem er sowohl die *Intensität* als auch das *Ausmaß* des Eingriffs betrachtet, was zu der Annahme führt, dass eine solche Beeinträchtigung eher quantitativ als qualitativ definiert wird. So hat der Gerichtshof zum einen im Urteil Digital Rights im Wesentlichen die Auffassung vertreten, dass die durch die Richtlinie 2006/24/EG [91] auferlegte Pflicht zur Vorratsspeicherung von Daten keinen solchen Schweregrad erreichte, dass sie sich auf den Wesensgehalt des Rechts auf Achtung des Privatlebens auswirken würde, da sie „die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen“ nicht gestattete [92]. Zum anderen ist der Gerichtshof im Gutachten 1/15 im Wesentlichen davon ausgegangen, dass eine Einschränkung, die auf bestimmte Aspekte des Privatlebens der betreffenden Personen beschränkt ist, nicht zu einem Eingriff in den Wesensgehalt dieses Grundrechts führen kann [93].

94. Was das Grundrecht auf Schutz personenbezogener Daten betrifft, so scheint der Gerichtshof die Ansicht zu vertreten, dass der Wesensgehalt dieses Rechts gewahrt ist, wenn die Maßnahme, die den Eingriff begründet, die Zwecke der Verarbeitung begrenzt und Regeln vorsieht, mit denen die Sicherheit der betreffenden Daten, insbesondere gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung, gewährleistet wird [94].

95. In der vorliegenden Rechtssache hat das vorlegende Gericht das Erfordernis der Achtung des Wesensgehalts der in den Art. 7 und 8 der Charta niedergelegten Rechte zwar nicht ausdrücklich erwähnt, die Frage der Einhaltung dieses Erfordernisses liegt nach meinem Dafürhalten aber der vierten und der sechsten Vorlagefrage zugrunde. Deshalb schlage ich dem Gerichtshof vor, darauf einzugehen.

96. In Rn. 150 des Gutachtens 1/15 hat der Gerichtshof insoweit zwar anerkannt, dass PNR-Daten „unter Umständen sehr genaue Informationen über das Privatleben einer Person liefern können“ [95] und diese Informationen möglicherweise direkt oder indirekt sensible Daten der betreffenden Person offenlegen [96], in Bezug auf den Entwurf eines PNR-Abkommens Kanada–EU gleichwohl aber den Schluss gezogen, dass, da die „Art dieser Informationen auf

90 Ich verweise insoweit auf die Erwägungen in der teilweise übereinstimmenden gemeinsamen Meinung der Richter Lemmens, Vehabović und Bošniak im Urteil Big Brother Watch (§§ 3 bis 10).

91 Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. 2006, L 105, S. 54).

92 Vgl. Urteil Digital Rights (Rn. 39); vgl. auch – in Bezug auf die Richtlinie 2002/58 – Urteil Tele2 Sverige (Rn. 101).

93 Vgl. Gutachten 1/15 (Rn. 150).

94 Vgl. in diesem Sinne u. a. Urteil Digital Rights (Rn. 40).

95 Vgl. in demselben Sinne Gutachten 1/15 (Rn. 128).

96 Vgl. Gutachten 1/15 (Rn. 164 und 165).

bestimmte Aspekte dieses Privatlebens beschränkt [ist], die insbesondere Flugreisen zwischen Kanada und der Union betreffen", die Verletzung des Grundrechts auf Achtung des Privatlebens nicht geeignet ist, den Wesensgehalt dieses Rechts zu beeinträchtigen.

97. Abgesehen von dem Umstand, dass die PNR-Daten, auf die sich der Entwurf eines PNR-Abkommens Kanada–EU bezieht, an einen Drittstaat übermittelt und von den Behörden dieses Drittstaats in dessen Hoheitsgebiet weiterverarbeitet werden mussten, stimmen die sich aus dem Abkommensentwurf ergebenden Eingriffe in das Grundrecht auf Achtung des Privatlebens und die in der PNR-Richtlinie vorgesehenen Eingriffe ihrem Wesen nach weitgehend überein. Dies gilt insbesondere für die genannten PNR-Daten, den systematischen und allgemeinen Charakter der Übermittlung und Verarbeitung dieser Daten, die Automatisierung der Verarbeitung sowie die Vorratsspeicherung der Daten. Was die beiden Rechtssachen hingegen unterscheidet, ist sozusagen die „geografische Abdeckung" dieser Eingriffe. Wie ich in Nr. 77 der vorliegenden Schlussanträge ausgeführt habe, sind die in der vorliegenden Rechtssache in Rede stehenden Datenverarbeitungen nämlich nicht auf Flugverbindungen mit einem einzigen Drittland beschränkt, wie es im Gutachten 1/15 der Fall war, sondern beziehen sich auf nahezu sämtliche Flüge in die Union und aus der Union sowie innerhalb der Union. Folglich müssen nach der PNR-Richtlinie – verglichen mit dem Entwurf eines PNR-Abkommens Kanada–EU – deutlich mehr Daten zu Fluggästen, die sich mit dem Flugzeug innerhalb und außerhalb der Union fortbewegen, systematisch verarbeitet werden. Außerdem ist ihre Verarbeitung angesichts der Zunahme der Menge verarbeiteter Daten und der Häufigkeit ihrer Erhebung vermutlich geeignet, sowohl genauere als auch umfassendere Informationen über das Privatleben der betreffenden Personen (Reisegewohnheiten, persönliche Beziehungen, finanzielle Situationen, usw.) zu liefern.

98. Gleichwohl beziehen sich diese Informationen, wie im Gutachten 1/15 der Fall, isoliert betrachtet nur auf bestimmte Aspekte des Privatlebens im Zusammenhang mit Flugreisen. Unter Berücksichtigung der Notwendigkeit, den Begriff „Wesensgehalt" der Grundrechte eng auszulegen, damit er seine Funktion eines Bollwerks gegen Angriffe auf die eigentliche Substanz dieser Rechte behält, bin ich jedoch der Ansicht, dass die Schlussfolgerung, zu der der Gerichtshof in Rn. 150 des Gutachtens 1/15 gelangt ist, auf die vorliegende Rechtssache übertragen werden kann.

99. Im Gutachten 1/15 hat der Gerichtshof auch eine Beeinträchtigung des Wesensgehalts des Rechts auf Schutz personenbezogener Daten ausgeschlossen[97]. Diese Schlussfolgerung ist aus meiner Sicht ebenfalls auf die Umstände der vorliegenden Rechtssache übertragbar. Wie der Entwurf eines PNR-Abkommens Kanada–EU begrenzt die PNR-Richtlinie in ihrem Art. 1 Abs. 2 nämlich die Zwecke der Verarbeitung von PNR-Daten. Darüber hinaus enthalten die PNR-Richtlinie und die anderen Unionsrechtsakte, auf die sie verweist, insbesondere die DSGVO und die Polizei-Richtlinie, spezifische Bestimmungen, mit denen insbesondere die Sicherheit, die Vertraulichkeit und die Integrität der Daten gewährleistet und diese vor unbefugten Zugriffen und unrechtmäßiger Verarbeitung geschützt werden sollen. Auch wenn nicht davon ausgegangen werden kann, dass eine Regelung wie die in der PNR-Richtlinie vorgesehene den Wesensgehalt der durch die Art. 7 und 8 der Charta geschützten Grundrechte antastet, muss sie gleichwohl einer strengen Verhältnismäßigkeitskontrolle unterworfen werden.

[97] Vgl. Gutachten 1/15 (Rn. 150).

c) Zur Einhaltung des Erfordernisses, wonach der Eingriff einer dem Gemeinwohl dienenden Zielsetzung entsprechen muss

100. Mit der PNR-Richtlinie soll u. a. für die innere Sicherheit der Union gesorgt und das Leben und die Sicherheit von Personen durch Übermittlung von PNR-Daten an die zuständigen Behörden der Mitgliedstaaten zur Verwendung im Rahmen der Bekämpfung des Terrorismus und schwerer Kriminalität geschützt werden [98].

101. Genauer gesagt geht aus Art. 1 Abs. 2 der PNR-Richtlinie in Verbindung mit deren Erwägungsgründen 6 und 7 sowie dem Vorschlag der Kommission, der zum Erlass dieser Richtlinie geführt hat (im Folgenden: Vorschlag für eine PNR-Richtlinie) [99], hervor, dass PNR-Daten von den Strafverfolgungsbehörden [100] im Rahmen eines solchen Ziels auf verschiedene Weise verwendet werden. Erstens werden diese Daten verwendet, um Personen zu identifizieren, die an bereits begangenen terroristischen Straftaten und bereits begangener schwerer Kriminalität beteiligt oder mutmaßlich beteiligt sind, Beweise zusammenzutragen sowie gegebenenfalls Komplizen von Straftätern aufzuspüren und kriminelle Netze auszuheben („reaktive" Verwendung). Zweitens können PNR-Daten vor Ankunft oder Abreise der Fluggäste ausgewertet werden, um die Begehung einer Straftat zu verhindern und Personen zu identifizieren, die bislang nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein, und die aufgrund des Auswertungsergebnisses von den Strafverfolgungsbehörden genauer überprüft werden sollten (Verwendung in „Echtzeit"). Schließlich werden PNR-Daten verwendet, um Prüfkriterien zu bestimmen, die für eine Überprüfung der Fluggäste vor ihrer Ankunft oder Abreise herangezogen werden können („proaktive" Verwendung). Durch eine solche proaktive Verwendung von PNR-Daten sollte es den Strafverfolgungsbehörden möglich sein, die Bedrohung durch schwere Kriminalität und Terrorismus anders anzugehen als durch Verarbeitung anderer Kategorien personenbezogener Daten [101].

102. Aus der Rechtsprechung des Gerichtshofs geht hervor, dass das Ziel des Schutzes der öffentlichen Sicherheit, das u. a. die Verhütung, Ermittlung, Feststellung und Verfolgung sowohl von terroristischen Straftaten als auch von Straftaten umfasst, die der schweren Kriminalität zuzuordnen sind, eine dem Gemeinwohl dienende Zielsetzung der Union im Sinne von Art. 52 Abs. 1 der Charta darstellt, die auch schwere Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte rechtfertigen kann [102].

103. Der Gerichtshof hat darüber hinaus anerkannt, dass die Ziele der Wahrung der öffentlichen Sicherheit und der Bekämpfung schwerer Kriminalität zum Schutz der Rechte und Freiheiten anderer beitragen [103]. So ist bei einer ausgewogenen Gewichtung dieser Ziele und den in den Art. 7 und 8 der Charta niedergelegten Grundrechten [104] auch die Bedeutung der in den

98 Vgl. u. a. Erwägungsgründe 5, 6, 15 und 22 der PNR-Richtlinie.

99 Vorschlag der Kommission vom 2. Februar 2011 über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (KOM[2011] 32 endg., S. 4).

100 Der Einfachheit halber werde ich in den vorliegenden Schlussanträgen den Ausdruck „Strafverfolgungsbehörden" verwenden, um allgemein jede Behörde zu bezeichnen, die mit Befugnissen in den von der PNR-Richtlinie erfassten Bereichen der Aufdeckung, Verhütung, Verfolgung oder Ermittlung von Terrorismus und schwerer Kriminalität ausgestattet ist.

101 Vgl. siebter Erwägungsgrund der PNR-Richtlinie. Vgl. auch Vorschlag für eine PNR-Richtlinie, S. 5.

102 Vgl. in diesem Sinne Gutachten 1/15 und Urteil vom 2. März 2021, Prokuratuur (Voraussetzungen für den Zugang zu Daten zu elektronischen Kommunikationen) (C-746/18, im Folgenden: Urteil Prokuratuur, EU:C:2021:152, Rn. 33 und die dort angeführte Rechtsprechung).

103 Vgl. in diesem Sinne Gutachten 1/15 (Rn. 149 und die dort angeführte Rechtsprechung) sowie Urteil La Quadrature du Net.

104 Vgl. im Folgenden Analyse zur Verhältnismäßigkeit des Eingriffs.

Art. 3, 4, 6 und 7 der Charta niedergelegten Rechte zu berücksichtigen. Im Urteil La Quadrature du Net hat der Gerichtshof insoweit zwar die Auffassung vertreten, dass Art. 6 der Charta „nicht dahin ausgelegt werden [kann], dass er die staatlichen Stellen verpflichtet, spezifische Maßnahmen zur Ahndung bestimmter Straftaten zu erlassen“ [105]; in Bezug insbesondere auf die wirksame Bekämpfung von Straftaten, deren Opfer u. a. Minderjährige und andere schutzbedürftige Personen sind, hat er hingegen hervorgehoben, dass sich aus Art. 7 der Charta positive Verpflichtungen der Behörden im Hinblick auf den Erlass rechtlicher Maßnahmen zum Schutz des Privat- und Familienlebens sowie aus deren Art. 3 und 4 hinsichtlich des Schutzes der körperlichen und geistigen Unversehrtheit der Menschen sowie des Verbots der Folter und unmenschlicher oder erniedrigender Behandlung ergeben können [106].

104. Schließlich ist der Gerichtshof davon ausgegangen, dass die Bedeutung des Ziels des Schutzes der *nationalen Sicherheit* die der Ziele, die Kriminalität im Allgemeinen, auch schwere Kriminalität, zu bekämpfen und die öffentliche Sicherheit zu schützen, übersteigt und dass es daher geeignet ist, Maßnahmen zu rechtfertigen, die schwerere Grundrechtseingriffe enthalten als solche, die mit den übrigen Zielen gerechtfertigt werden könnten [107]. Da terroristische Handlungen Bedrohungen der nationalen Sicherheit der Mitgliedstaaten darstellen können, trägt das mit der PNR-Richtlinie geschaffene System, soweit es als Instrument zur Bekämpfung solcher Handlungen dient, zum Ziel des Schutzes der nationalen Sicherheit der Mitgliedstaaten bei.

d) Zur Wahrung des Grundsatzes der Verhältnismäßigkeit

105. Nach Art. 52 Abs. 1 Satz 2 der Charta dürfen Einschränkungen der Ausübung eines in der Charta anerkannten Grundrechts unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

106. Insoweit ist darauf hinzuweisen, dass der Grundsatz der Verhältnismäßigkeit nach ständiger Rechtsprechung des Gerichtshofs verlangt, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist [108].

107. Nach ständiger Rechtsprechung des Gerichtshofs verlangt der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das *absolut Notwendige* beschränken. Außerdem kann eine dem Gemeinwohl dienende Zielsetzung nicht verfolgt werden, ohne den Umstand zu berücksichtigen, dass sie mit den von der Maßnahme betroffenen Grundrechten in Einklang gebracht werden muss, indem eine ausgewogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen wird [109]. Insbesondere ist die Verhältnismäßigkeit einer Beschränkung der in den Art. 7 und 8 der Charta niedergelegten

105 Vgl. Urteil La Quadrature du Net (Rn. 125).

106 Vgl. Urteil La Quadrature du Net (Rn. 126 und die dort angeführte Rechtsprechung).

107 Vgl. Urteil La Quadrature du Net (Rn. 136).

108 Vgl. Urteil Digital Rights (Rn. 46 und die dort angeführte Rechtsprechung).

109 Vgl. Gutachten 1/15 (Rn. 140 und die dort angeführte Rechtsprechung) sowie Urteil La Quadrature du Net (Rn. 130 und die dort angeführte Rechtsprechung). Das Erfordernis, dass die Verarbeitung personenbezogener Daten in allen Phasen der Verarbeitung ein „ausgewogenes Verhältnis zwischen allen betroffenen Interessen, seien sie öffentlich oder privat, und den betroffenen Rechten und Freiheiten“ widerspiegelt, wird auch in Art. 5 des Übereinkommens Nr. 108 aufgestellt.

Rechte zu beurteilen, indem die Schwere des mit einer solchen Beschränkung verbundenen Eingriffs bestimmt und geprüft wird, ob die verfolgte dem Gemeinwohl dienende Zielsetzung in angemessenem Verhältnis zur Schwere des Eingriffs steht [110].

108. Aus der Rechtsprechung des Gerichtshofs geht hervor, dass die PNR-Richtlinie als Rechtsgrundlage, mit der die in den Nrn. 70 bis 83 der vorliegenden Schlussanträge beschriebenen Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte verbunden sind, um dem Erfordernis der Verhältnismäßigkeit zu genügen, klare und präzise Regeln für die Tragweite und die Anwendung der Maßnahmen, die solche Eingriffe enthalten, vorsehen und Mindesterfordernisse aufstellen muss, so dass die Personen, deren Daten übermittelt wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen [111]. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten, wie im vorliegenden Fall, automatisch verarbeitet werden und es um den Schutz der besonderen Kategorie sensibler personenbezogener Daten geht [112].

109. Was den Umfang der gerichtlichen Überprüfung der Einhaltung der sich aus dem Grundsatz der Verhältnismäßigkeit ergebenden Erfordernisse anbelangt, so ist der Gestaltungsspielraum des Unionsgesetzgebers angesichts der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens und des mit der PNR-Richtlinie verbundenen Eingriffs in dieses Recht eingeschränkt, so dass die Kontrolle strikt sein muss [113].

1) Zur Eignung der in der PNR-Richtlinie vorgesehenen Verarbeitungen von PNR-Daten für die Verwirklichung des verfolgten Ziels

110. Wie der Gerichtshof in Rn. 153 des Gutachtens 1/15 in Bezug auf den Entwurf eines PNR-Abkommens Kanada–EU festgestellt hat, kann davon ausgegangen werden, dass die Übermittlung der PNR-Daten an Kanada und ihre anschließende Verarbeitung geeignet sind, die Verwirklichung des Ziels des Schutzes der öffentlichen Sicherheit zu gewährleisten. Diese Eignung, die sowohl auf Unionsebene als auch auf globaler Ebene seit langem anerkannt ist [114], scheint mir in Bezug auf die Erhebung und Weiterverarbeitung von PNR-Daten zu Drittstaatsflügen und EU-Flügen nicht in Frage gestellt werden zu können [115].

111. Allerdings muss die Wirksamkeit des mit der Richtlinie geschaffenen Systems zur Verarbeitung von PNR-Daten durch eine Beurteilung der Ergebnisse seiner Anwendung konkret bewertet werden [116]. Unter diesem Blickwinkel ist es von wesentlicher Bedeutung, dass die

110 Vgl. in diesem Sinne Urteil vom 2. Oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, Rn. 55 und die dort angeführte Rechtsprechung), sowie Urteile La Quadrature du Net (Rn. 131) und Prokuratuur (Rn. 32).

111 Vgl. in diesem Sinne Urteile Digital Rights (Rn. 54) und Schrems I (Rn. 91) sowie Gutachten 1/15 (Rn. 141).

112 Vgl. Gutachten 1/15 (Rn. 141 und die dort angeführte Rechtsprechung).

113 Vgl. in diesem Sinne Urteil Digital Rights (Rn. 48).

114 Vgl. in diesem Sinne Nrn. 201 bis 203 der vorliegenden Schlussanträge.

115 Ich verweise insoweit auf die im Arbeitspapier von 2020 enthaltenen Daten.

116 Vgl. in diesem Sinne Stellungnahme vom 19. August 2016, S. 5.

Wirksamkeit Gegenstand einer kontinuierlichen Bewertung auf der Grundlage möglichst präziser und zuverlässiger statistischer Daten ist [117]. Die Kommission sollte insoweit regelmäßig eine Überprüfung analog zu der bereits in Art. 19 der PNR-Richtlinie vorgesehenen vornehmen.

2) Zur absoluten Notwendigkeit des Eingriffs

112. Obwohl der Verfassungsgerichtshof nicht ausdrücklich daran gezweifelt hat, dass die PNR-Richtlinie klare, präzise und auf das absolut Notwendige beschränkte Regeln für die Abgrenzung der Zwecke der Verarbeitungen von PNR-Daten enthält [118], muss bei der vom vorlegenden Gericht erbetenen Prüfung der Verhältnismäßigkeit des in dieser Richtlinie vorgesehenen Systems nach meinem Dafürhalten darauf eingegangen werden [119].

i) Zur Abgrenzung der Zwecke der Verarbeitung von PNR-Daten

113. Eine klare Abgrenzung der Zwecke, für die der Zugang zu personenbezogenen Daten und ihre anschließende Verwendung durch die zuständigen Behörden zulässig sind, stellt eine grundlegende Anforderung an jedes System zur Verarbeitung von Daten insbesondere zu Strafverfolgungszwecken dar. Diese Anforderung muss darüber hinaus erfüllt sein, damit der Gerichtshof die Verhältnismäßigkeit der in Rede stehenden Maßnahmen beurteilen kann, indem er die in seiner Rechtsprechung entwickelte Prüfung des Verhältnisses zwischen der Schwere des Eingriffs und der verfolgten Zielsetzung anwendet [120].

114. Der Gerichtshof hat u. a. im Urteil Digital Rights, in dem er die Richtlinie 2006/24 für ungültig erklärt hat, hervorgehoben, welche Bedeutung eine klare Abgrenzung der Zwecke von Maßnahmen hat, die mit Einschränkungen der Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten verbunden sind. In Rn. 60 dieses Urteils hat der Gerichtshof festgestellt, dass die Richtlinie 2006/24 „kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken, die im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in Art. 7 und Art. 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen“, und sie im Gegenteil „in ihrem Art. 1 Abs. 1 lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten schweren Straftaten Bezug [nimmt]“.

115. Art. 1 Abs. 2 der PNR-Richtlinie stellt ein allgemeines Kriterium zur Abgrenzung der Zwecke auf, wonach „[d]ie nach Maßgabe dieser Richtlinie erhobenen PNR-Daten … ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität … verarbeitet werden [dürfen]“. Im Gegensatz zur Richtlinie 2006/24 beschränkt sich die PNR-Richtlinie jedoch nicht auf das Aufstellen eines solchen Kriteriums, sondern definiert selbst in ihrem Art. 3 Nrn. 8 und 9 sowohl

[117] Zur Bedeutung von Statistiken für die Beurteilung der Effizienz des mit der PNR-Richtlinie geschaffenen Systems vgl. u. a. Gutachten 1/2011 vom 14. Juni 2011 betreffend den Vorschlag für eine PNR-Richtlinie, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_DE.pdf, Nr. 2.1.2.1 (im Folgenden: FRA-Gutachten 1/2011).

[118] Diese Frage wird vom Verwaltungsgericht Wiesbaden (Deutschland) in der anhängigen Rechtssache C-215/20 hingegen deutlich gestellt.

[119] Die Kommission ist im Rahmen einer zur schriftlichen Beantwortung gestellten Frage aufgefordert worden, hierzu Stellung zu nehmen. Die übrigen Verfahrensbeteiligten haben in der mündlichen Verhandlung Stellung nehmen können.

[120] Vgl. Nr. 107 a. E. der vorliegenden Schlussanträge.

den Begriff „terroristische Straftaten“ als auch den Begriff „schwere Kriminalität“, Ersteren unter Verweis auf die Art. 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. 2002, L 164, S. 3) (ersetzt durch die Richtlinie [EU] 2017/541)[121] und Letzteren, indem zum einen in Anhang II die Kategorien von strafbaren Handlungen aufgeführt werden, die diesem Begriff entsprechen, und zum anderen eine Erheblichkeitsschwelle eingeführt wird, die sich nach der Höchstdauer der Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung richtet, mit der diese Straftaten bedroht sind.

116. Auch wenn sich die Handlungen, die gemäß Art. 3 Nr. 8 der PNR-Richtlinie als terroristische Straftaten eingestuft werden können, durch den Verweis auf die einschlägigen Bestimmungen der Richtlinie 2017/541 hinreichend klar und präzise kennzeichnen lassen und ihre Schwere für die Zwecke der Abwägung zwischen dem mit der PNR-Richtlinie verfolgten Ziel des Schutzes der öffentlichen Sicherheit und der Schwere des mit dieser Richtlinie verbundenen Eingriffs in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte beurteilt werden kann, gilt das nicht ohne Weiteres für alle in Anhang II aufgeführten strafbaren Handlungen.

117. In Rn. 177 des Gutachtens 1/15 hat der Gerichtshof die Auffassung vertreten, dass der Entwurf eines PNR-Abkommens Kanada–EU klar und präzise den Schweregrad von Straftaten, auf die sich der Begriff „grenzübergreifende schwere Kriminalität“ bezieht, definiert, indem er verlangt, dass diese Straftaten „mit einer Freiheitsstrafe im Höchstmaß von mindestens vier Jahren oder mit einer schwereren Strafe geahndet“ werden, auf „die Straftaten nach kanadischem Recht“ Bezug nimmt und „die verschiedenen Fälle [aufführt], in denen eine Straftat als grenzübergreifend gilt“.

118. Im Vergleich zu der vom Gerichtshof im Gutachten 1/15 untersuchten Regelung berücksichtigt die PNR-Richtlinie bei der Definition der in Bezug genommenen strafbaren Handlungen erstens nicht deren grenzübergreifenden Charakter, sieht zweitens einen erschöpfenden Katalog strafbarer Handlungen vor, die ihrem Wesen nach als der schweren Kriminalität zugehörig angesehen werden, sofern sie die in Art. 3 Nr. 9 der Richtlinie vorgesehene Mindesthöchststrafe erreichen, und senkt drittens grundsätzlich die Erheblichkeitsschwelle, indem sie ein auf der Dauer der Höchststrafe beruhendes Kriterium wählt und diese Schwelle auf drei Jahre festsetzt.

119. Was erstens das Fehlen eines auf dem grenzübergreifenden Charakter beruhenden Abgrenzungskriteriums angeht, so trifft es zwar zu, dass auf strafbare Handlungen, die ihrem Wesen nach zumindest potenziell eine objektive Verbindung zu Flugreisen und daher zu den nach der PNR-Richtlinie erhobenen und verarbeiteten Datenkategorien unterhalten könnten, hätte abgezielt werden können, wenn der sachliche Anwendungsbereich dieser Richtlinie allein auf „grenzübergreifende“ schwere Kriminalität begrenzt worden wäre[122]. Ich teile jedoch grundsätzlich den Standpunkt der Kommission, wonach die Relevanz und Notwendigkeit eines solchen Kriteriums bei einer Regelung zur Kriminalitätsbekämpfung, deren Ziel darin besteht, die innere Sicherheit der Union zu schützen, weniger auf der Hand liegt als im Kontext eines

[121] Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. 2017, L 88, S. 6).

[122] Ich stelle insoweit fest, dass der Begriff „Straftat mit grenzübergreifendem Charakter“, wie er beispielsweise im Entwurf eines PNR-Abkommens Kanada–EU definiert wird, weit genug war, um auch in einem Land verübte Straftaten einzuschließen, bei deren Begehung sich der Straftäter „in einem anderen Land aufhält oder dorthin ausreisen will“; vgl. Art. 3 Abs. 3 Buchst. e des Entwurfs eines PNR-Abkommens Kanada–EU, dessen Wortlaut in Rn. 30 des Gutachtens 1/15 wiedergegeben wird. Ich stelle ferner fest, dass die FRA in ihrem Gutachten 1/2011 (Nrn. 2.2.3.1 und 3.7) vorgeschlagen hatte, das PNR-System der EU auf schwere grenzüberschreitende Kriminalität zu beschränken. Der Vorschlag für eine PNR-Richtlinie zog hingegen eine differenzierte automatisierte Verarbeitung für grenzüberschreitende und nicht grenzüberschreitende Kriminalität in Betracht (vgl. Art. 4 Abs. 2 Buchst. a dieses Vorschlags).

internationalen Übereinkommens. Darüber hinaus ist das Fehlen grenzüberschreitender Elemente, wie die Kommission weiter vorträgt, als solches kein Anhaltspunkt für den Ausschluss der Schwere einer Straftat.

120. Was zweitens das Kriterium zur Festlegung der Erheblichkeitsschwelle für die in Bezug genommenen Straftaten betrifft, die, um eine *Ex-ante*-Beurteilung dieser Schwere zu ermöglichen, dahin ausgelegt werden muss, dass sie sich auf die Höchstdauer der gesetzlich vorgesehenen Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung und nicht auf die Dauer bezieht, die in einem bestimmten Fall konkret drohen könnte, so ist dieses Kriterium, obwohl es auf der Mindesthöchststrafe und nicht auf dem Mindestmaß der Mindeststrafe beruht, als solches nicht ungeeignet, einen hinreichenden Schweregrad zu identifizieren, der den mit dem in der PNR-Richtlinie vorgesehenen Datenverarbeitungen verbundenen Eingriff in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte rechtfertigen könnte. Aus meiner Sicht ist es jedoch wie ein Kriterium zur Identifizierung eines „Mindestschweregrads" auszulegen. Daher verbietet ein solches Kriterium den Mitgliedstaaten zwar, in Anhang II aufgeführte Straftaten, für die ihr nationales Strafrecht eine Freiheitsstrafe oder freiheitsentziehende Maßregel der Sicherung mit einer Höchstdauer von weniger als drei Jahren vorsieht, als „schwere Kriminalität" anzusehen, verpflichtet sie jedoch nicht dazu, für alle Straftaten, die in Anhang II aufgenommen werden könnten und mit einer Strafe bedroht sind, die die in Art. 3 Nr. 9 der PNR-Richtlinie vorgesehene Schwelle erreicht, automatisch eine solche Einstufung vorzunehmen, wenn diese unter Berücksichtigung der Besonderheiten ihres Strafrechtssystems zu einer Anwendung der in der PNR-Richtlinie vorgesehenen Regelung für Zwecke der Verhütung, Aufdeckung, Ermittlung oder Verfolgung gemeinschaftlich begangener Straftaten führt, die den mit dieser Richtlinie verfolgten Zwecken zuwiderläuft.

121. Drittens ist zum Katalog von Anhang II zunächst zu bemerken, dass der Umstand, dass die PNR-Richtlinie die strafbaren Handlungen, die unter die Definition der „schweren Kriminalität" fallen, abschließend aufführt, eine grundlegende förmliche und substanzielle Garantie darstellt, damit die Rechtmäßigkeit des mit der PNR-Richtlinie geschaffenen Systems und die Rechtssicherheit der Fluggäste gewährleistet sind. Festzustellen ist jedoch, dass der Katalog sowohl strafbare Handlungen, die ihrem Wesen nach einen unbestreitbar hohen Schweregrad aufweisen – wie beispielsweise Menschenhandel, sexuelle Ausbeutung von Kindern und Kinderpornografie, illegalen Handel mit Waffen oder nuklearen bzw. radioaktiven Substanzen, Flugzeug- und Schiffsentführung, Verbrechen, die in die Zuständigkeit des Internationalen Strafgerichtshofs fallen, vorsätzliche Tötung, Vergewaltigung sowie Entführung, Freiheitsberaubung und Geiselnahme[123] –, als auch Straftaten einschließt, für die ein solcher Schweregrad weniger offensichtlich ist, etwa Betrugsdelikte, betrügerische Nachahmung und

[123] Ein Teil der in Anhang II aufgeführten strafbaren Handlungen fällt darüber hinaus in Kriminalitätsbereiche, die von Art. 83 Abs. 1 Unterabs. 1 AEUV als „besonders schwer" eingestuft werden und in Unterabs. 2 dieses Absatzes aufgeführt sind. Es handelt sich u. a. um Menschenhandel, sexuelle Ausbeutung von Kindern, illegalen Drogenhandel, illegalen Waffenhandel, Geldwäsche, Korruption, Fälschung von Zahlungsmitteln, Computerkriminalität und organisierte Kriminalität. In mehreren dieser Bereiche hat der Unionsgesetzgeber auf der Grundlage von Art. 83 Abs. 1 AEUV Richtlinien mit „Mindestvorschriften zur Festlegung von Straftaten und Strafen" erlassen; vgl. u. a. Richtlinie 2011/36/EU des Europäischen Parlaments und des Rates vom 5. April 2011 zur Verhütung und Bekämpfung des Menschenhandels und zum Schutz seiner Opfer sowie zur Ersetzung des Rahmenbeschlusses 2002/629/JI des Rates (ABl. 2011, L 101, S. 1), Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. 2011, L 335, S. 1), Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. 2013, L 218, S. 8), Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. 2019, L 123, S. 18), Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug (ABl. 2017, L 198, S. 29) und Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die strafrechtliche Bekämpfung der Geldwäsche (ABl. 2018, L 284, S. 22).

Produktpiraterie, Fälschung von amtlichen Dokumenten und Handel damit sowie Handel mit gestohlenen Kraftfahrzeugen [124]. Darüber hinaus sind von den in Anhang II aufgenommenen strafbaren Handlungen einige ihrem Wesen nach eher geeignet als andere, grenzüberschreitenden Charakter aufzuweisen, etwa Menschenhandel, illegaler Handel mit Drogen oder Waffen, sexuelle Ausbeutung von Kindern, Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt sowie Flugzeugentführung, und gleichzeitig in einem Zusammenhang mit dem Passagierluftverkehr zu stehen.

122. Auch hinsichtlich der hinreichenden Klarheit und Präzision der Rubriken in Anhang II ist das Niveau sehr variabel. So haben, obwohl die in diesem Anhang enthaltene Liste als erschöpfend angesehen werden muss, mehrere ihrer Rubriken „offenen" Charakter [125], während andere auf generische Begriffe verweisen, die eine sehr große Anzahl strafbarer Handlungen unterschiedlichen Schweregrads einschließen können, wenn auch stets innerhalb der Grenze des in Art. 3 Nr. 9 der PNR-Richtlinie vorgesehenen maximalen Schwellenwerts [126].

123. Zum einen liefern die in den Bereichen von Art. 83 Abs. 1 AEUV erlassenen und in Fn. 123 der vorliegenden Schlussanträge erwähnten Harmonisierungsrichtlinien insoweit relevante Anhaltspunkte, mit denen sich zumindest einige der schweren Straftaten identifizieren lassen, die in die entsprechenden Rubriken von Anhang II fallen könnten. So definiert u. a. die Richtlinie 2013/40 in ihren Art. 3 bis 8 verschiedene Straftaten, die dem in Anhang II Nr. 9 genannten Begriff der „Computerkriminalität" zuzuordnen sind, wobei sie in jedem einzelnen Fall dafür Sorge trägt, Handlungen auszuschließen, die „leichte Fälle" darstellen [127]. Auch die Richtlinie 2019/713 definiert bestimmte Typologien von Betrugsdelikten, und die Richtlinie 2017/1371 legt die Tatbestandsmerkmale eines „gegen die finanziellen Interessen der Union gerichteten Betrugs" fest. In diesem Zusammenhang ist auch die auf der Grundlage von Art. 175 Abs. 1 EG erlassene Richtlinie 2008/99/EG über den strafrechtlichen Schutz der Umwelt [128] zu erwähnen, die in ihrem Art. 3 eine Reihe schwerer Umweltstraftaten definiert, die in die Rubrik 10 von Anhang II aufgenommen werden könnten, einschließlich Handlungen, die als „illegaler Handel mit bedrohten Tierarten oder mit bedrohten Pflanzen- und Baumarten" eingestuft werden können, wobei sie alle Handlungen ausschließt, die unerhebliche Auswirkungen auf das geschützte Gut haben. Ich weise schließlich auf die Richtlinie 2002/90/EG [129], die die Beihilfe zur unerlaubten Ein- und Durchreise und zum unerlaubten Aufenthalt definiert, sowie auf den Rahmenbeschluss 2002/946/JI [130] betreffend die Verstärkung des strafrechtlichen Rahmens für die Bekämpfung

124 Alle in Anhang II aufgeführten strafbaren Handlungen mit Ausnahme der „Wirtschaftsspionage" sind jedoch in Art. 2 Abs. 2 des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. 2002, L 190, S. 1) enthalten. Auch wenn sie nicht ausdrücklich als schwer eingestuft werden, führen sie, wenn sie die Schwelle erreichen, die in Art. 3 Nr. 9 der PNR-Richtlinie für eine freiheitsentziehende Maßregel der Sicherung vorgesehen ist, ohne Überprüfung des Vorliegens der beiderseitigen Strafbarkeit gleichwohl zur Übergabe aufgrund eines Europäischen Haftbefehls. Nahezu alle aufgeführten Straftaten mit Ausnahme der „Sabotage", der „Flugzeugentführung" und der „Wirtschaftsspionage" sind auch in Anhang I der Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates (ABl. 2018, L 295, S. 138) enthalten, der alle „Formen schwerer Kriminalität" aufzählt, für die Eurojust zuständig ist.

125 Es handelt sich insbesondere um die Nrn. 7, 8, 10 und 16.

126 Dies ist beispielsweise bei den „Betrugsdelikten" (Nr. 7), der „Korruption" (Nr. 6), der „Computerkriminalität" (Nr. 9) und der „Umweltkriminalität" (Nr. 10) der Fall. In der anhängigen Rechtssache C-215/20 hegt das Verwaltungsgericht Wiesbaden insbesondere Bedenken wegen der Betrugsdelikte.

127 Diese Richtlinie legt in ihrem Art. 9 im Übrigen die Mindestdauer der Höchstfreiheitsstrafe fest, mit der die genannten Straftaten geahndet werden müssen – eine Schwelle, die nur unter bestimmten Umständen drei Jahre erreicht.

128 Richtlinie des [Europäischen] Parlaments und des Rates vom 19. November 2008 (ABl. 2008, L 328, S. 28).

129 Richtlinie des Rates vom 28. November 2002 zur Definition der Beihilfe zur unerlaubten Ein- und Durchreise und zum unerlaubten Aufenthalt (ABl. 2002, L 328, S. 17).

130 Rahmenbeschluss des Rates vom 28. November 2002 betreffend die Verstärkung des strafrechtlichen Rahmens für die Bekämpfung der Beihilfe zur unerlaubten Ein- und Durchreise und zum unerlaubten Aufenthalt (ABl. 2002, L 328, S. 1).

dieser Straftaten, den Rahmenbeschluss 2003/568/JI [131], der Straftaten definiert, die als „Bestechung und Bestechlichkeit im privaten Sektor" eingestuft werden, und den Rahmenbeschluss 2008/841/JI [132] hin, der Straftaten definiert, die sich auf die Beteiligung an einer kriminellen Vereinigung beziehen.

124. Zum anderen kann dem Unionsgesetzgeber, worauf die Kommission zu Recht hingewiesen hat, ohne eine vollständige Harmonisierung des materiellen Strafrechts nicht vorgeworfen werden, die in Anhang II aufgeführten strafbaren Handlungen nicht weiter präzisiert zu haben. So verlangt die Umsetzung des Katalogs der strafbaren Handlungen von Anhang II in innerstaatliches Recht – anders als es weiter unten in den vorliegenden Schlussanträgen in Bezug auf die in Anhang I enthaltene Liste der PNR-Daten festgestellt werden wird – notwendigerweise von den Mitgliedstaaten, dass sie die Straftaten, die aufgeführt werden könnten, nach Maßgabe der Besonderheiten ihrer nationalen Strafrechtssysteme definieren. Dieser Vorgang hat jedoch unter voller Achtung des Kriteriums zu erfolgen, wonach jeder Eingriff in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte auf das absolut Notwendige beschränkt werden muss. So können die Mitgliedstaaten nach meinem Dafürhalten beispielsweise vorsehen, dass die Verwendung von PNR-Daten bei bestimmten Straftaten wie z. B. den in Anhang II Nrn. 7, 16, 17, 18 und 25 aufgeführten strafbaren Handlungen auf Fälle beschränkt wird, in denen diese Straftaten grenzübergreifenden Charakter aufweisen, im Rahmen einer kriminellen Vereinigung begangen werden oder bestimmte erschwerende Umstände umfassen. Die Gerichte der Mitgliedstaaten werden die nationalen Vorschriften, mit denen der besagte Katalog in innerstaatliches Recht umgesetzt wird, unter der Kontrolle des Gerichtshofs im Einklang sowohl mit der PNR-Richtlinie als auch mit der Charta auszulegen haben, so dass die Verarbeitung von PNR-Daten bei jeder Rubrik auf strafbare Handlungen, die den von dieser Richtlinie geforderten hohen Schweregrad erreichen, und auf strafbare Handlungen beschränkt bleibt, für die eine solche Verarbeitung maßgeblich ist [133].

125. Vorbehaltlich der Ausführungen in den Nrn. 120 und 124 der vorliegenden Schlussanträge bin ich der Ansicht, dass Art. 3 Nr. 9 der PNR-Richtlinie und der in deren Anhang II enthaltene Straftatenkatalog den Erfordernissen der Klarheit und Präzision genügen und nicht über die Grenzen des absolut Notwendigen hinausgehen.

126. Es ist jedoch einzuräumen, dass die in Nr. 124 der vorliegenden Schlussanträge dargestellte Lösung nicht vollkommen zufriedenstellend ist. Zum einen belässt sie den Mitgliedstaaten nämlich einen beträchtlichen Ermessensspielraum, so dass der sachliche Anwendungsbereich der Verarbeitung von PNR-Daten von einem Mitgliedstaat zum anderen erheblich variieren kann, wodurch das vom Unionsgesetzgeber verfolgte Harmonisierungsziel beeinträchtigt wird [134]. Zum anderen bedeutet sie, dass die Verhältnismäßigkeitskontrolle über ein wesentliches Element des Systems wie die Begrenzung der Zwecke dieser Verarbeitung eher *ex post* über die nationalen Umsetzungsmaßnahmen als *ex ante* über die PNR-Richtlinie selbst ausgeübt wird. Es wäre daher wünschenswert, wenn der Gerichtshof, sollte er beschließen, wie ich es ihm zu tun vorschlage, Art. 3 Nr. 9 der PNR-Richtlinie und den in deren Anhang II enthaltenen Straftatenkatalog als im Einklang mit den Art. 7, 8 und 52 Abs. 1 der Charta stehend anzusehen, den Unionsgesetzgeber darauf hinweist, dass eine solche Beurteilung nur vorläufig ist und der Unionsgesetzgeber im Licht der Umsetzung dieser Vorschrift und dieses Katalogs durch die Mitgliedstaaten sowie auf der Grundlage der in Art. 20 der PNR-Richtlinie genannten statistischen Daten überprüfen muss,

131 Rahmenbeschluss des Rates vom 22. Juli 2003 zur Bekämpfung der Bestechung im privaten Sektor (ABl. 2003, L 192, S. 54).

132 Rahmenbeschluss des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität (ABl. 2008, L 300, S. 42).

133 Vgl. u. a. Erwägungsgründe 7 und 22 der PNR-Richtlinie.

134 Vgl. 35. Erwägungsgrund der PNR-Richtlinie.

ob es erforderlich ist, i) die in besagtem Katalog aufgeführten Kategorien strafbarer Handlungen durch eine Eingrenzung ihrer Tragweite weiter zu präzisieren, ii) Straftaten aus ihm zu streichen, für die sich die Verarbeitung von PNR-Daten als unverhältnismäßig, d. h. irrelevant oder unwirksam, erweist, und iii) die Schwelle der Erheblichkeit bei den in Art. 3 Nr. 9 der PNR-Richtlinie aufgeführten strafbaren Handlungen anzuheben [135]. Ich stelle insoweit fest, dass Art. 19 Abs. 2 Buchst. b der PNR-Richtlinie die Kommission zwar dazu verpflichtet, alle Elemente dieser Richtlinie zu überprüfen und dabei insbesondere „die Erforderlichkeit und Verhältnismäßigkeit der Erhebung und Verarbeitung von PNR-Daten für jeden der in [der] Richtlinie genannten Zwecke“ zu berücksichtigen, weder der Bericht der Kommission von 2020 noch das ihm beigefügte Arbeitspapier von 2020 nach meinem Dafürhalten diesbezüglich aber eine zufriedenstellende Prüfung enthalten.

ii) Zu den Kategorien von PNR-Daten, auf die sich die PNR-Richtlinie bezieht (zweite und dritte Vorlagefrage)

127. Die PNR-Richtlinie sieht die Übermittlung von 19 Kategorien von PNR-Daten, die von den Fluggesellschaften für Buchungszwecke erhoben werden, an die PNR-Zentralstellen vor. Diese Kategorien, die in Anhang I aufgeführt sind, entsprechen denen, die in den Buchungssystemen der Fluggesellschaften erscheinen, und denen, die in Anhang I der von der Internationalen Zivilluftfahrt-Organisation (ICAO) im Jahr 2010 angenommenen Leitlinien zu Fluggastdatensätzen [136] (im Folgenden: ICAO-Leitlinien) aufgeführt sind.

128. Mit seiner zweiten Vorlagefrage möchte das vorlegende Gericht erfahren, ob Anhang I im Hinblick auf die Art. 7, 8 und 52 Abs. 1 der Charta gültig ist, wenn zum einen der Umfang der in diesem Anhang aufgeführten personenbezogenen Daten – insbesondere der in dessen Nr. 18 genannten API-Daten, soweit sie über die in Art. 3 Abs. 2 der API-Richtlinie aufgeführten Daten hinausgehen – und zum anderen der Umstand berücksichtigt wird, dass diese Daten zusammengenommen möglicherweise sensible Daten offenlegen und so die Grenzen des „absolut Notwendigen“ überschreiten. Mit seiner dritten Vorlagefrage – die sich, wie ich bereits hervorgehoben habe, auf die Einhaltung der ersten der drei in Art. 52 Abs. 1 der Charta genannten Voraussetzungen bezieht, wonach jeder Eingriff in ein Grundrecht „gesetzlich vorgesehen“ sein muss – befragt der Verfassungsgerichtshof den Gerichtshof hingegen zur Gültigkeit von Anhang I Nrn. 12 und 18 unter besonderer Berücksichtigung des „offenen“ Charakters dieser Nummern.

129. Da die im Rahmen der zweiten Vorlagefrage durchzuführende Prüfung die Prüfung der Frage voraussetzt, ob die in Anhang I aufgeführten Kategorien personenbezogener Daten hinreichend klar und präzise sind, werde ich zunächst auf die dritte Vorlagefrage eingehen.

135 Vgl. entsprechend Urteile vom 16. Dezember 2008, Arcelor Atlantique und Lorraine u. a. (C-127/07, EU:C:2008:728, Rn. 61 und 62), sowie vom 17. Oktober 2013, Schaible (C-101/12, EU:C:2013:661, Rn. 91 und 94).

136 Vgl. Dokument 9944, gebilligt und veröffentlicht vom Generalsekretär der ICAO. Die französische Sprachfassung dieses Dokuments ist zugänglich auf der Website https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf. Gemäß Anhang 9 (Erleichterungen) Nr. 9.22 des am 7. Dezember 1944 in Chicago unterzeichneten Abkommens über die internationale Zivilluftfahrt (im Folgenden: Abkommen von Chicago) sind die Vertragsstaaten des Abkommens, die PNR-Daten verlangen, verpflichtet, ihren Bedarf an Daten und die Verarbeitung dieser Daten u. a. an die Leitlinien anzupassen.

– *Zur hinreichenden Klarheit und Präzision von Anhang I Nrn. 12 und 18 (dritte Vorlagefrage)*

130. Einleitend ist zu bemerken, dass das Ausmaß und die Schwere des Eingriffs in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte, der mit einer Maßnahme zur Einführung von Einschränkungen der Ausübung dieser Rechte verbunden ist, vor allem vom Umfang und von der Art der personenbezogenen Daten abhängen, die Gegenstand der Verarbeitung sind. Die Identifizierung dieser Daten stellt somit einen wichtigen Arbeitsschritt dar, der für jede Rechtsgrundlage, mit der eine solche Maßnahme eingeführt wird, zwingend auf möglichst klare und präzise Weise vorgenommen werden muss.

131. Dieses Erfordernis ist in Bezug auf die Verarbeitung von PNR-Daten durch das Gutachten 1/15 anerkannt worden. Der Gerichtshof hat sich in diesem Gutachten zu den Rubriken im Anhang des Entwurfs eines PNR-Abkommens Kanada–EU, in dem die PNR-Daten aufgeführt sind, auf die sich das geplante Abkommen bezieht, geäußert und u. a. die Auffassung vertreten, dass allgemeine Kategorien von Informationen, die den Umfang der zu übermittelnden Daten nicht hinreichend bestimmen, sowie beispielhafte Datenlisten, die keinerlei Einschränkung hinsichtlich der Art und des Umfangs der Informationen festlegen, die in der betreffenden Rubrik enthalten sein könnten, die Voraussetzungen der Klarheit und Präzision nicht erfüllen.

132. Im Licht dieser Grundsätze ist die dritte Vorlagefrage zu prüfen.

133. Anhang I Nr. 12 hat folgenden Wortlaut:

„Allgemeine Hinweise (einschließlich aller verfügbaren Angaben zu unbegleiteten Minderjährigen unter 18 Jahren, wie beispielsweise Name und Geschlecht des Minderjährigen, Alter, Sprache(n), Name und Kontaktdaten der Begleitperson beim Abflug und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, Name und Kontaktdaten der abholenden Person und Angabe, in welcher Beziehung diese Person zu dem Minderjährigen steht, begleitender Flughafenmitarbeiter bei Abflug und Ankunft)“.

134. Soweit sie sich auf „allgemeine Hinweise“ bezieht, handelt es sich bei dieser Nummer – wie bei Rubrik 17 des Anhangs des Entwurfs eines PNR-Abkommens Kanada–EU – um eine sogenannte „free text“-Rubrik, mit der über die in den übrigen Nummern von Anhang I ausdrücklich angeführten Informationen hinaus jede Information einbezogen werden soll, die von den Fluggesellschaften im Rahmen ihrer Dienstleistungstätigkeit erhoben wird. Festzustellen ist jedoch, wie es der Gerichtshof in Rn. 160 des Gutachtens 1/15 getan hat, dass eine derartige Rubrik „keine Angaben über Art und Umfang der zu übermittelnden Informationen [enthält] und … selbst Informationen umfassen [könnte], die keinerlei Bezug zum Zweck der Übermittlung der PNR-Daten haben“. Da die im Wortlaut von Anhang I Nr. 12 enthaltene Erläuterung in Klammern, die sich auf Informationen über unbegleitete Minderjährige bezieht, lediglich beispielhaft erfolgt, wie aus der Verwendung des Wortes „einschließlich“ hervorgeht, begrenzt sie Art und Umfang der Informationen, die von ihr erfasst werden können, nicht [137].

135. Anhang I Nr. 12 ist mithin nicht hinreichend klar und präzise abgegrenzt.

[137] Vgl. in demselben Sinne Gutachten 1/15 (Rn. 160).

136. Während die Kommission und das Parlament diese Schlussfolgerung zu teilen scheinen, treten ihr die Mitgliedstaaten, die Erklärungen zur dritten Vorlagefrage abgegeben haben, und der Rat entgegen, und zwar auf der Grundlage von Argumentationen, die sich weitgehend überschneiden.

137. Als Erstes soll mit einer ersten Reihe von Argumenten allgemein in Frage gestellt werden, dass die Schlussfolgerungen, zu denen der Gerichtshof im Gutachten 1/15 gelangt ist, auf die vorliegende Rechtssache übertragen werden können.

138. Auch wenn ich mir des unterschiedlichen Kontexts der beiden Rechtssachen bewusst bin, beschränke ich mich hier insoweit auf die Feststellung, dass die Schlussfolgerung, zu der der Gerichtshof in Rn. 160 des Gutachtens 1/15 in Bezug auf Rubrik 17 des Anhangs des Entwurfs eines PNR-Abkommens Kanada–EU gelangt ist, auf einer rein semantischen und strukturellen Auslegung dieser Rubrik beruhte. Eine solche Auslegung ist ohne Weiteres auf Anhang I Nr. 12 übertragbar, dessen Wortlaut hinsichtlich des nicht beispielhaften Teils mit dem Wortlaut der besagten Rubrik identisch ist und eine ähnliche Struktur aufweist. Darüber hinaus fügen sich die beiden in Rede stehenden Vorschriften, wie nachstehend ausgeführt werden soll, in den gleichen multilateralen Regelungskontext ein, der u. a. aus den ICAO-Leitlinien besteht, auf die sich der Gerichtshof in Rn. 156 des Gutachtens 1/15 im Übrigen ausdrücklich bezogen hat. Unter diesen Umständen steht nicht nur nichts einer Auslegung von Anhang I Nr. 12 entgegen, wie sie der Gerichtshof in Rn. 160 des Gutachtens 1/15 in Bezug auf Rubrik 17 des Anhangs des Entwurfs eines PNR-Abkommens Kanada–EU vorgenommen hat, sondern rechtfertigt vor allem nichts ihre Aufgabe.

139. Als Zweites hebt ein Großteil der Mitgliedstaaten hervor, dass die verschiedenen Nummern von Anhang I, einschließlich Nr. 12, den Rubriken von Anhang I der ICAO-Leitlinien entsprächen, die den Fluggesellschaften gut bekannt seien und denen sie ohne Weiteres einen präzisen Inhalt zuweisen könnten. Nr. 12 entspreche insbesondere den letzten beiden Rubriken des besagten Anhangs, die mit „Allgemeine Eintragungen“ bzw. „Freitext/Codefelder in OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], Eintragungen/Historien“ überschrieben seien und sich auf „zusätzliche Angaben“ bzw. „Angaben über geforderte Dienstleistungen“ bezögen [138].

140. Hierzu weise ich zunächst darauf hin, dass die Übereinstimmung zwischen den Rubriken von Anhang I des Entwurfs eines PNR-Abkommens Kanada–EU einerseits und den Rubriken von Anhang I der ICAO-Leitlinien andererseits den Gerichtshof nicht daran gehindert hat, im Gutachten 1/15 festzustellen, dass einige der in Anhang I des Entwurfs eines Abkommens enthaltenen Rubriken nicht die Anforderungen der Klarheit und Präzision erfüllen, denen eine Maßnahme zur Einschränkung der Ausübung von Grundrechten genügen muss. Sodann lassen sich Art und Umfang der Informationen, die von Anhang I Nr. 12 erfasst werden könnten, anders als einige Mitgliedstaaten offenbar meinen, mit einem – im Übrigen nicht ausdrücklichen [139] – Verweis auf die ICAO-Leitlinien nicht weiter präzisieren. Im Gegenteil: Bei

[138] Vgl. Nrn. 2.1.2 und 2.1.5 der ICAO-Leitlinien.

[139] Die einzige Bezugnahme auf die ICAO-Leitlinien in der PNR-Richtlinie ist in deren 17. Erwägungsgrund enthalten und betrifft lediglich die „unterstützten Datenformate für die Übermittlung von PNR-Daten durch die Fluggesellschaften an die Mitgliedstaaten“.

einer Lektüre dieser Leitlinien wird die Schlussfolgerung bestätigt, wonach eine „free text"-Rubrik wie Nr. 12 über die von Amts wegen in den PNR-Daten enthaltenen Informationen hinaus eine unbestimmte Zahl von Informationen unterschiedlichster Art einschließt [140].

141. Als Drittes tragen einige Regierungen vor, es sei Sache der Mitgliedstaaten, im Wege innerstaatlicher gesetzgeberischer Maßnahmen und unter Beachtung der durch die Art. 7, 8 und 52 Abs. 1 der Charta auferlegten Grenzen zu präzisieren, welche Informationen in Anhang I Nr. 12 enthalten sein könnten. Es gehöre nämlich zum Wesen einer Richtlinie, den Mitgliedstaaten einen Ermessensspielraum hinsichtlich der notwendigen Mittel zur Umsetzung der Richtlinienbestimmungen zu belassen.

142. Wie ich bereits in Nr. 86 der vorliegenden Schlussanträge dargelegt habe, bin ich insoweit der Ansicht, dass es, wenn Maßnahmen, die mit Eingriffen in die in der Charta niedergelegten Grundrechte verbunden sind, ihren Ursprung in einem Gesetzgebungsakt der Union haben, dem Unionsgesetzgeber obliegt, unter Achtung der vorerwähnten Kriterien der Klarheit und Präzision sowie unter Wahrung des Grundsatzes der Verhältnismäßigkeit die genaue Tragweite dieser Eingriffe festzulegen. Ist das vom Unionsgesetzgeber gewählte Instrument eine Richtlinie, kann den Mitgliedstaaten bei der Umsetzung dieser Richtlinie in ihre nationalen Rechtsordnungen nach meinem Dafürhalten folglich nicht die Bestimmung wesentlicher Elemente zur Festlegung der Tragweite des Eingriffs wie beispielsweise – was Einschränkungen der in den Art. 7 und 8 der Charta niedergelegten Grundrechte anbelangt – Art und Umfang der verarbeiteten personenbezogenen Daten übertragen werden.

143. Als Viertes weisen einige Mitgliedstaaten darauf hin, dass Anhang I Nr. 12 so zu verstehen sei, dass sich diese Nummer lediglich auf Informationen beziehe, die mit der Beförderungsleistung zusammenhingen. So ausgelegt, sei die Nummer mit den Art. 7, 8 und 52 Abs. 1 der Charta vereinbar.

144. Auch dieses Argument überzeugt mich nicht. Denn zunächst sind Informationen, die von einer Rubrik „Allgemeine Hinweise" sowie unter den Codes OSI, SSI und SSR erfasst werden können, sehr heterogener Natur (medizinische Betreuung, Spezialverpflegung oder Ernährungspräferenzen, jedwede Unterstützungsanfragen, Informationen über allein reisende Minderjährige, usw.) [141] und weisen allesamt insofern einen Zusammenhang mit der Beförderungsleistung auf, als der Fluggesellschaft mit ihnen u. a. ermöglicht werden soll, diese Leistung an die Erfordernisse der einzelnen Fluggäste anzupassen. Mit einem Auslegungskriterium, das auf der Relevanz der Information für die Beförderungsleistung beruht, ließe sich die Tragweite von Anhang I Nr. 12 somit nicht weiter präzisieren. Sodann hat der Gerichtshof in Rn. 159 des Gutachtens 1/15 zwar auf dieses Kriterium zurückgegriffen, um eine andere Rubrik des Anhangs des Entwurfs eines PNR-Abkommens Kanada–EU im Einklang mit den Erfordernissen der Klarheit und Präzision auszulegen, gleichwohl aber ausgeschlossen, in Bezug auf Rubrik 17 dieses Anhangs, der Anhang I Nr. 12 entspricht, so vorgehen zu können.

145. Als Fünftes haben manche Mitgliedstaaten unterstrichen, dass die Angaben, die in Anhang I Nr. 12 aufgeführt sein sollten, den Fluggesellschaften von den ordnungsgemäß über die spätere Übermittlung dieser Daten an die öffentlichen Stellen informierten Fluggästen selbst freiwillig

[140] So ist in Nr. 2.1.5 der ICAO-Leitlinien von „zusätzlichen Angaben" bzw. „Angaben über geforderte Dienstleistungen" die Rede, die sich „auf Anträge auf medizinische Betreuung oder Spezialverpflegung, ‚allein reisende Minderjährige', Unterstützungsanfragen, usw." beziehen können. In Nr. 2.1.6 heißt es wiederum, dass das „Feld ‚Allgemeine Erläuterungen'" auch „bestimmte Angaben wie beispielsweise die Korrespondenz oder den internen Schriftverkehr zwischen dem Personal der Fluggesellschaften und den Reservierungsmitarbeitern" enthalten kann.

[141] Vgl. Nrn. 2.1.5 und 2.1.6 der ICAO-Leitlinien.

gemacht würden. Diesem Argument scheint der Gedanke zugrunde zu liegen, dass es eine Art stillschweigender Einwilligung des betreffenden Fluggasts in die Weiterleitung der den Fluggesellschaften mitgeteilten Daten an die öffentlichen Stellen gebe.

146. Der Gerichtshof hat insoweit bereits klargestellt, dass von einer „Einwilligung" keine Rede sein kann, wenn sich die betreffende Person der Verarbeitung ihrer personenbezogenen Daten nicht frei widersetzen kann [142]. Bei einem Großteil der Angaben, die von Anhang I Nr. 12 erfasst werden können, hat der betroffene Fluggast jedoch keine wirkliche Wahl, sondern ist verpflichtet, sie zu machen, um die Beförderungsleistung in Anspruch nehmen zu können. Dies gilt insbesondere für Personen mit Behinderungen oder eingeschränkter Mobilität oder für Personen, die medizinische Betreuung benötigen, oder aber für unbegleitete Minderjährige. Darüber hinaus kann, wie der Gerichtshof in den Rn. 142 und 143 des Gutachtens 1/15 eindeutig festgestellt hat, nicht davon ausgegangen werden, dass Verarbeitungen von PNR-Daten durch öffentliche Stellen, mit denen ein anderer Zweck verfolgt wird als der, für den die Daten von den Fluggesellschaften erhoben wurden, irgendeine Form von Einwilligung der Fluggäste zu dieser Erhebung zugrunde liegt.

147. Schließlich macht die Mehrzahl der Mitgliedstaaten geltend, die in der PNR-Richtlinie vorgesehenen Datenverarbeitungen seien mit zahlreichen Schutzvorkehrungen versehen, zu denen – was die Übermittlung von Daten an die PNR-Zentralstellen angehe – deren Verpflichtung gehöre, nicht in Anhang I enthaltene Daten und Daten, aus denen die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihr Gesundheitszustand, ihr Sexualleben oder ihre sexuelle Orientierung hervorgehen könnten, zu löschen.

148. Dazu ist zunächst zu sagen, dass die Beurteilung der hinreichenden Klarheit und Präzision von Regeln zur Festlegung des Umfangs und der Art der Daten, die Gegenstand einer Übermittlung an die öffentlichen Stellen sein können, soweit sie gewährleisten soll, dass eine Maßnahme, die mit Eingriffen in die in den Art. 7 und 8 der Charta niedergelegten Rechte verbunden ist, die Grundsätze der Gesetzmäßigkeit und der Rechtssicherheit wahrt, vorgenommen werden muss, ohne den Schutzvorkehrungen Rechnung zu tragen, die mit den Verarbeitungen einhergehen, denen die Daten von den öffentlichen Stellen unterworfen werden sollen, da diese Schutzvorkehrungen erst bei der Prüfung der Verhältnismäßigkeit der in Rede stehenden Maßnahme berücksichtigt werden. Im Übrigen hat der Gerichtshof die Rubriken des Entwurfs eines PNR-Abkommens Kanada–EU in den Rn. 155 bis 163 des Gutachtens 1/15 auf diese Weise beurteilt. Zudem sollte auf die Notwendigkeit, die verschiedenen Phasen der Prüfung einer mit Grundrechtseingriffen verbundenen Maßnahme deutlich voneinander abzugrenzen, da eine Verquickung zwischen den verschiedenen Phasen nach meinem Dafürhalten stets auf Kosten eines effektiven Grundrechtsschutzes geht, ganz allgemein besonderes Augenmerk gelegt werden.

149. Abgesehen davon beschränke ich mich hier auf die Feststellung, dass die den PNR-Zentralstellen gemäß Art. 6 Abs. 1 der PNR-Richtlinie obliegende Verpflichtung, andere als die in Anhang I genannten Daten zu löschen, nur Sinn macht, wenn dieser Anhang einen klaren und geschlossenen Katalog zu übermittelnder Daten enthält. Gleiches gilt für die den PNR-Zentralstellen gemäß Art. 13 Abs. 4 der PNR-Richtlinie obliegende Verpflichtung,

[142] Vgl. Urteil vom 17. Oktober 2013, Schwarz (C-291/12, EU:C:2013:670, Rn. 32), das sich auf den Fall der einen Reisepass beantragenden Person bezieht, die verpflichtet ist, sich der Erfassung ihrer Fingerabdrücke zu unterziehen, um über ein Dokument verfügen zu können, das es ihr ermöglicht, in ein Drittland zu reisen.

sogenannte „sensible“ Daten [143] zu löschen. Eine zu vage, ungenaue oder offene Definition der Informationen, die übermittelt werden müssen, erhöht nämlich sowohl die Wahrscheinlichkeit, dass solche Daten indirekt übermittelt werden, als auch das Risiko, dass sie nicht sogleich identifiziert und gelöscht werden. Mit anderen Worten können die vorerwähnten Schutzvorkehrungen ihre Funktion nur sinnvoll erfüllen, wenn die Regeln zur Festlegung von Art und Umfang der PNR-Daten, die die Fluggesellschaften den PNR-Zentralstellen zu übermitteln haben, hinreichend klar und präzise sind und die Liste mit diesen Daten geschlossenen und erschöpfenden Charakter hat.

150. Nach alledem bin ich, wie ich in Nr. 135 der vorliegenden Schlussanträge vorweggenommen habe, der Ansicht, dass Anhang I Nr. 12 hinsichtlich des Teils, in dem „allgemeine Hinweise“ zu den Daten gezählt werden, die die Fluggesellschaften den PNR-Zentralstellen gemäß der PNR-Richtlinie zu übermitteln haben, den sich aus Art. 52 Abs. 1 der Charta in der Auslegung durch den Gerichtshof ergebenden Erfordernissen der Klarheit und Präzision nicht genügt [144] und daher insoweit für ungültig erklärt werden sollte.

151. In ihren schriftlichen Erklärungen haben die Kommission und das Parlament dem Gerichtshof vorgeschlagen, eher auf eine „richtlinienkonforme Auslegung“ von Anhang I Nr. 12 zurückzugreifen und diese Nummer dahin zu verstehen, dass sie sich nur auf die darin ausdrücklich in Klammern erwähnten Angaben zu Minderjährigen bezieht. Ich gebe zu, dass ich mit der Auffassung, wonach eine solche Lesart die Grenzen einer einfachen richtlinienkonformen Auslegung respektiere, gewisse Schwierigkeiten habe. Es trifft zwar zu, dass ein Unionsrechtsakt nach einem allgemeinen Auslegungsgrundsatz so weit wie möglich in einer seine Gültigkeit nicht in Frage stellenden Weise und im Einklang mit dem gesamten Primärrecht und insbesondere mit den Bestimmungen der Charta auszulegen ist [145]. Es ist auch richtig, dass die Möglichkeit einer solchen Auslegung in Bezug auf die PNR-Richtlinie durch den Schwerpunkt, den u. a. zahlreiche Erwägungsgründe dieser Richtlinie auf die uneingeschränkte Wahrung der Grundrechte, des Rechts auf Achtung des Privatlebens und des Grundsatzes der Verhältnismäßigkeit legen [146], befürwortet zu werden scheint. Es ist jedoch ebenfalls ständige Rechtsprechung, dass eine richtlinienkonforme Auslegung nur zulässig ist, wenn die Vorschrift des abgeleiteten Unionsrechts mehr als eine Auslegung zulässt und es daher möglich ist, die Auslegung, bei der die Bestimmung mit dem Primärrecht vereinbar ist, derjenigen vorzuziehen, die zur Feststellung ihrer Unvereinbarkeit mit diesem führt [147].

152. Anhang I Nr. 12 kann nach meinem Dafürhalten nicht so ausgelegt werden, wie die Kommission und das Parlament vorschlagen, wenn diese Nummer nicht „*contra legem*“ ausgelegt werden soll. Sie bezieht sich nämlich, wie ich oben dargelegt habe, auf eine große Kategorie unterschiedlichster Arten von Daten, die nicht im Voraus bestimmbar sind und verglichen mit den Daten zu Minderjährigen nur eine Unterkategorie darstellen. Eine Auslegung der Nummer dahin gehend, dass sie sich nur auf diese Unterkategorie bezieht, liefe nicht nur darauf hinaus,

143 Auf diese Datenkategorie werde ich weiter unten in den vorliegenden Schlussanträgen zurückkommen.

144 Die FRA hat sich in ihrem Gutachten 1/2011 (S. 13) in diesem Sinne geäußert. In seiner Stellungnahme vom 25. März 2011 zum Vorschlag für eine PNR-Richtlinie (https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_de.pdf, Nr. 47) (im Folgenden: Stellungnahme des EDSB vom 25. März 2011) hat der EDSB vorgeschlagen, die Rubrik „Allgemeine Hinweise“ von der Liste des Anhangs I zu entfernen.

145 Vgl. u. a. Urteile vom 19. November 2009, Sturgeon u. a. (C-402/07 und C-432/07, EU:C:2009:716, Rn. 47 und die dort angeführte Rechtsprechung), vom 19. September 2013, Überprüfung Kommission/Strack (C-579/12 RX-II, EU:C:2013:570, Rn. 40), sowie vom 14. Mai 2019, M u. a. (Aberkennung der Flüchtlingseigenschaft) (C-391/16, C-77/17 und C-78/17, EU:C:2019:403, Rn. 77 und die dort angeführte Rechtsprechung).

146 Vgl. u. a. Erwägungsgründe 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 und 37 der PNR-Richtlinie.

147 Vgl. Urteile vom 26. Juni 2007, Ordre des barreaux francophones et germanophone u. a. (C-305/05, EU:C:2007:383, Rn. 28), sowie vom 14. Mai 2019, M u. a. (Aberkennung der Flüchtlingseigenschaft) (C-391/16, C-77/17 und C-78/17, EU:C:2019:403, Rn. 77).

einen Teil ihres Wortlauts außer Acht zu lassen, sondern würde auch dessen logische Ordnung untergraben. Ein derartiges Vorgehen, das im Wesentlichen darin besteht, den Teil des Wortlauts von Anhang I Nr. 12 zu entfernen, der als nicht im Einklang mit den Erfordernissen der Klarheit und Präzision stehend angesehen würde, ist nach meinem Dafürhalten nur bei einer teilweisen Nichtigerklärung möglich.

153. Der verbleibende Teil von Anhang I Nr. 12, in dem eine Reihe von Daten zu unbegleiteten Minderjährigen aufgeführt ist, genügt meiner Ansicht nach den Erfordernissen der Klarheit und Präzision, sofern er dahin ausgelegt wird, dass er nur Angaben zu unbegleiteten Minderjährigen umfasst, die unmittelbar mit dem Flug zusammenhängen und in dieser Nummer ausdrücklich genannt sind.

154. Anhang I Nr. 18 hat folgenden Wortlaut:

„Etwaige erhobene erweiterte Fluggastdaten (API-Daten) (einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten, Staatsangehörigkeit, Familienname, Vorname, Geschlecht, Geburtsdatum, Fluggesellschaft, Flugnummer, Tag des Abflugs, Tag der Ankunft, Flughafen des Abflugs, Flughafen der Ankunft, Uhrzeit des Abflugs und Uhrzeit der Ankunft)“.

155. Diese Nummer weist eine Struktur auf, die derjenigen von Anhang I Nr. 12 ähnlich ist. Auch in ihr wird eine allgemeine Datenkategorie erwähnt, nämlich erweitere Fluggastdaten (Advance Passenger Information – API), gefolgt von – in Klammern – einer Liste mit Daten, die als in diese allgemeine Kategorie fallend angesehen werden, wobei die Liste lediglich eine nicht abschließende Aufzählung enthält, wie die Verwendung des Wortes „einschließlich“ belegt.

156. Im Gegensatz zu Anhang I Nr. 12 verweist Anhang I Nr. 18 jedoch auf eine Kategorie von Daten, die sowohl hinsichtlich ihrer Art als auch hinsichtlich ihres Umfangs besser identifizierbar sind. Aus dem vierten Erwägungsgrund der PNR-Richtlinie geht nämlich hervor, dass die Richtlinie, wenn sie sich auf diese Datenkategorie bezieht, auf Informationen abstellt, die von den Fluggesellschaften gemäß der API-Richtlinie, auf die der Erwägungsgrund ausdrücklich verweist, als Mittel zur Verbesserung der Grenzkontrollen und zur Bekämpfung der illegalen Einwanderung vorab an die zuständigen nationalen Behörden übermittelt werden. Diese Daten sind aufgeführt in Art. 3 Abs. 2 der letztgenannten Richtlinie.

157. Aus dem neunten Erwägungsgrund [148] der PNR-Richtlinie sowie aus Art. 3 Abs. 2 der API-Richtlinie und der in Anhang I Nr. 18 enthaltenen Beispielliste geht ferner hervor, dass es sich bei den API-Daten, auf die sich diese Nummer bezieht, zum einen um biografische Daten, mit denen sich die Identität des Fluggasts überprüfen lässt, und zum anderen um Daten zum gebuchten Flug handelt. Was insbesondere die erste Kategorie – die der biografischen Daten –

[148] Soweit hier relevant, sieht der neunte Erwägungsgrund vor: „Die Verwendung von PNR-Daten zusammen mit API-Daten bietet einen Mehrwert, indem sie den Mitgliedstaaten die Feststellung der Identität einer Person erleichtert, mithin den Nutzen dieses Ergebnisses für die Verhütung, Aufdeckung und Ermittlung von Straftaten erhöht und die Gefahr minimiert, dass Überprüfungen und Ermittlungen zu unschuldigen Personen durchgeführt werden.“

betrifft, so umfassen die in Art. 3 Abs. 2 der API-Richtlinie und Anhang I Nr. 18 aufgeführten Informationen beim Check-in erzeugte Daten, die dem maschinenlesbaren Teil eines Reisepasses (oder anderen Reisedokuments) entnommen werden können [149].

158. Somit wird mit Anhang I Nr. 18, ausgelegt im Licht der Erwägungsgründe 4 und 9 der PNR-Richtlinie, grundsätzlich zumindest die Art der Daten, auf die sich diese Nummer bezieht, hinreichend klar und präzise bezeichnet.

159. Zu ihrem Umfang ist zum einen festzustellen, dass auch Art. 3 Abs. 2 der API-Richtlinie „offen" gefasst ist, da der darin enthaltenen Datenliste die Wendung „zu diesen Daten zählen" vorausgeht [150], und zum anderen, dass in der Kategorie der API-Daten, wie sie in den einschlägigen multilateralen Harmonisierungsinstrumenten definiert wird, auch Daten enthalten sind, die nicht zu den Daten gehören, auf die sich sowohl die API-Richtlinie als auch Anhang I Nr. 18 beziehen [151].

160. Damit Anhang I Nr. 18 den Erfordernissen der Klarheit und Präzision genügt, die für Rechtsgrundlagen gelten, die Eingriffe in die Art. 7 und 8 der Charta enthalten, ist diese Nummer daher dahin auszulegen, dass sie nur die in ihr und in Art. 3 Abs. 2 der API-Richtlinie ausdrücklich genannten API-Daten erfasst, die von den Fluggesellschaften im Rahmen ihrer normalen Geschäftstätigkeit erhoben worden sind [152].

161. An dieser Stelle soll ein kurzer Überblick über die anderen Nummern von Anhang I gegeben werden, die unter Berücksichtigung ihres Wortlauts ebenfalls einen „offenen" Charakter aufweisen oder nicht präzise genug sind, obwohl das vorlegende Gericht den Gerichtshof nicht ausdrücklich dazu befragt hat [153].

162. Was zunächst Anhang I Nr. 5 betrifft, so ist zwar davon auszugehen, dass sich diese Nummer, in der von „Anschrift und Kontaktangaben (Telefonnummer, E-Mail-Adresse)" die Rede ist, nur auf die in Klammern ausdrücklich erwähnten Kontaktangaben bezieht und somit erschöpfenden Charakter hat; in ihr wird jedoch nicht klargestellt, wie es bei der entsprechenden Rubrik des Entwurfs eines PNR-Abkommens Kanada–EU der Fall war [154], ob sich diese Kontaktangaben nur auf den Fluggast oder auch auf Dritte beziehen, die die Buchung des Fluges für den Fluggast vorgenommen haben, über die ein Fluggast erreicht werden kann oder die im

149 Vgl. in diesem Sinne auch Vorschlag für eine PNR-Richtlinie, S. 7 (Nr. 1). Dieselben Daten finden sich in den von der Weltzollorganisation (WZO), dem Verband des Internationalen Luftverkehrs (IATA) und der ICAO erarbeiteten Richtlinien über vorab übermittelte Fluggastdaten http://www.wcoomd.org/~/media/wco/public/fr/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/api-guidelines-_f.pdf?db=web) ([im Folgenden: Richtlinien über vorab übermittelte Fluggastdaten], Nr. 8.1.5 Buchst. a) als „wesentliche Datenelemente, die in der maschinenlesbaren Zone der amtlichen Reisedokumente enthalten sein können".

150 Art. 3 Abs. 2 der API-Richtlinie hat folgenden Wortlaut: „Zu diesen Angaben zählen: die Nummer und die Art des mitgeführten Reisedokuments, die Staatsangehörigkeit, der vollständige Name, das Geburtsdatum, die Grenzübergangsstelle für die Einreise in das Hoheitsgebiet der Mitgliedstaaten, die Beförderungs-Codenummer, die Abreise- und Ankunftszeit, die Gesamtzahl der mit der betreffenden Beförderung beförderten Personen, der ursprüngliche Abreiseort." Ich möchte betonen, dass die Kommission in ihrem Arbeitsprogramm für 2022 (KOM[2021] 645 endg., S. 9) eine Überarbeitung der API-Richtlinie ins Auge gefasst hat. Im September 2020 hat sie eine die Grundlage für ihre künftige Revision darstellende Bewertung der Richtlinie veröffentlicht, SWD(2020) 174 endg. (im Folgenden: Arbeitspapier von 2020 zur API-Richtlinie). In diesem Papier hebt die Kommission u. a. hervor, dass die in Art. 3 Abs. 2 der API-Richtlinie enthaltene Datenliste insbesondere insoweit nicht mit den internationalen Standards für API-Daten übereinstimme, als sie nicht alle Daten im maschinenlesbaren Teil der Identitätsdokumente einschließe (vgl. u. a. S. 48).

151 Vgl. Richtlinien über vorab übermittelte Fluggastdaten, Nr. 8.1.5 Buchst. b und c.

152 Eine ähnliche Auslegung der entsprechenden Rubrik des Entwurfs eines PNR-Abkommens Kanada–EU ist in Rn. 161 des Gutachtens 1/15 enthalten.

153 Der Gerichtshof ist derzeit mit einer Reihe von Vorlagefragen befasst, die sich speziell darauf beziehen, ob mehrere Nummern von Anhang I, insbesondere die Nrn. 4, 8, 12 und 18, hinreichend präzise sind (vgl. anhängige Rechtssache C-215/20).

154 Vgl. Gutachten 1/15 (Rn. 158).

Notfall zu verständigen sind [155]. Unter Berücksichtigung der Tatsache, dass der mit der PNR-Richtlinie verbundene Eingriff bei einer Auslegung von Anhang I Nr. 5 dahin gehend, dass sich diese Nummer auch auf die vorerwähnten Kategorien von Dritten bezieht, auf andere Subjekte als Fluggäste im Sinne von Art. 3 Nr. 4 der PNR-Richtlinie erstreckt würde, schlage ich dem Gerichtshof in Ermangelung genauer Daten, die die Annahme zulassen, dass die systematische und generalisierte Erfassung der Kontaktangaben dieser Dritten ein Element darstellt, das für die Wirksamkeit des mit der Richtlinie geschaffenen Systems zur Verarbeitung von PNR-Daten absolut notwendig ist, vor, die besagte Nummer so auszulegen, dass sie sich nur auf die darin ausdrücklich erwähnten Kontaktangaben zum Fluggast bezieht, in dessen Namen die Buchung getätigt wird. Zwar schließt die PNR-Richtlinie nicht aus, dass auch personenbezogene Daten anderer Subjekte als Fluggäste an die PNR-Zentralstellen übermittelt werden können [156]. Es ist jedoch äußerst wichtig, dass Sachverhalte, wo immer das möglich ist, klar und explizit benannt werden, wie es bei den in Anhang I Nr. 9 erwähnten Reisevermittlern oder bei den Begleitpersonen allein reisender Minderjähriger der Fall ist, auf die sich Anhang I Nr. 12 bezieht. Nur wenn die vorstehende Voraussetzung erfüllt ist, kann nämlich davon ausgegangen werden, dass die Entscheidung, diese Daten in die an die PNR-Zentralstellen zu übermittelnden Daten aufzunehmen, Gegenstand einer Abwägung der verschiedenen auf dem Spiel stehenden Interessen im Sinne des 15. Erwägungsgrundes der PNR-Richtlinie gewesen ist und die betreffenden Dritten angemessen über die Verarbeitung ihrer personenbezogenen Daten informiert werden können.

163. Was sodann Anhang I Nr. 6 betreffend „[a]lle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift“ angeht, so muss diese Nummer, um die Anforderungen an Klarheit und Präzision zu erfüllen, analog zu den vom Gerichtshof in Rn. 159 des Gutachtens 1/15 getroffenen Feststellungen zur entsprechenden Rubrik des Anhangs des Entwurfs eines PNR-Abkommens Kanada–EU dahin ausgelegt werden, dass sie „lediglich Informationen über die Modalitäten der Zahlung und die Abrechnung des Flugtickets betrifft, nicht aber andere Informationen, die keinen direkten Bezug zum Flug aufweisen“. Diese Informationen dürfen daher beispielsweise keine Informationen über die Modalitäten der Bezahlung anderer Leistungen umfassen, die nicht unmittelbar mit dem Flug verknüpft sind, wie die Miete eines Fahrzeugs bei der Ankunft [157].

164. Nr. 8, die den „Vielflieger-Eintrag“ betrifft, wird durch die ICAO-Normen als sich auf die Kontonummer oder den Vielfliegerstatus beziehend definiert [158]. So ausgelegt, genügt diese Nummer den Erfordernissen der Klarheit und Präzision.

165. Anhang I Nr. 10 („Reisestatus des Fluggasts mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge [No show] und Fluggäste mit Flugschein, aber ohne Reservierung [Go show]“) und Nr. 13 („Flugscheindaten einschließlich Flugscheinnummer, Ausstellungsdatum, einfacher Flug [One-way], automatische Tarifanzeige [Automated Ticket Fare Quote fields]“) beziehen sich trotz ihres offenen Wortlauts nur auf sehr präzise und eindeutig bestimmbare Informationen, die unmittelbar mit dem Flug zusammenhängen. Dies gilt auch für Anhang I Nr. 14 („Sitzplatznummer und sonstige Sitzplatzinformationen“) und Nr. 16 („Vollständige Gepäckangaben“).

155 Informationen über das Reisebüro oder den Sachbearbeiter werden bereits von Anhang I Nr. 5 erfasst.

156 Vgl. Definition von PNR-Daten in Art. 3 Nr. 5 der PNR-Richtlinie.

157 Vgl. in diesem Sinne auch Schlussanträge des Generalanwalts Mengozzi im Gutachten 1/15, ([PNR-Abkommen EU–Kanada], EU:C:2016:656), Nr. 218.

158 Vgl. entsprechende Rubrik von Anhang I der ICAO-Leitlinien.

– *Zum Umfang der in Anhang I aufgeführten Daten (zweite Vorlagefrage)*

166. Zu den Elementen, die der Gerichtshof bei der Beurteilung der Verhältnismäßigkeit einer Maßnahme berücksichtigt, die mit Eingriffen in die in den Art. 7 und 8 der Charta niedergelegten Rechte verbunden ist, gehört, dass die verarbeiteten personenbezogenen Daten angemessen, erheblich und nicht übermäßig sind (Grundsatz der „Datenminimierung“) [159]. Der gleiche Test ist nach der Rechtsprechung des EGMR üblich [160] und wird im Übereinkommen Nr. 108 empfohlen [161].

167. Aus dem 15. Erwägungsgrund der PNR-Richtlinie ergibt sich, dass die Liste mit den PNR-Daten, die für die PNR-Zentralstellen bestimmt sind, erstellt und inhaltlich so zusammengesetzt worden ist, dass sie durch die Anwendung „hoher Standards“, die mit der Charta, dem Übereinkommen Nr. 108 und der EMRK im Einklang stehen, sowohl den legitimen Bedürfnissen der Behörden im Zusammenhang mit der Bekämpfung des Terrorismus und schwerer Kriminalität gerecht wird als auch die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten schützt. Derselbe Erwägungsgrund stellt klar, dass die PNR-Daten u. a. nur jene Details über den Buchungsvorgang und die Reiseroute von Fluggästen beinhalten sollten, mit deren Hilfe die zuständigen Stellen diejenigen Fluggäste ermitteln können, die eine Bedrohung für die innere Sicherheit darstellen.

168. Was als Erstes die Angemessenheit und Erheblichkeit der PNR-Daten in Anhang I angeht, so beziehen sich die verschiedenen Nummern dieses Anhangs, einschließlich der Nrn. 5, 6, 8 und 18, wie ich sie auszulegen vorschlage [162], sowie der Nr. 12 mit Ausnahme des Teils, den ich für ungültig zu erklären vorschlage [163], nur auf Daten, die Informationen liefern, die in einem unmittelbaren Zusammenhang mit den in den Anwendungsbereich der PNR-Richtlinie fallenden Flugreisen stehen. Diese Daten sind außerdem objektiv mit den von der Richtlinie verfolgten Zwecken verknüpft. Insbesondere können API-Daten u. a. „reaktiv“ verwendet werden, um eine Person zu identifizieren, die den Strafverfolgungsbehörden bereits bekannt ist, beispielsweise weil sie im Verdacht steht, an bereits begangenen terroristischen Straftaten oder bereits begangener schwerer Kriminalität beteiligt zu sein, oder eine solche Straftat mutmaßlich begehen wird, während PNR-Daten eher in „Echtzeit oder proaktiv“ verwendet werden können, um Bedrohungen zu erkennen, die von Personen ausgehen, die den Strafverfolgungsbehörden noch nicht bekannt sind.

169. Was als Zweites den Umfang der in Anhang I aufgeführten PNR-Daten betrifft, so erscheinen diese Daten, einschließlich derjenigen in den Nrn. 5, 6, 8, 12 und 18, wie ich sie in den Nrn. 134 bis 164 der vorliegenden Schlussanträge auszulegen vorschlage, unter Berücksichtigung der Bedeutung des mit der PNR-Richtlinie verfolgten Ziels der öffentlichen Sicherheit einerseits und der Eignung des mit dieser Richtlinie geschaffenen Systems für die Verfolgung eines solchen Ziels andererseits nicht übermäßig.

159 Vgl. in diesem Sinne u. a. Urteil Digital Rights (Rn. 57). Zu dem Erfordernis, dass sich die Datenkategorien, auf die sich eine Zugangsmaßnahme bezieht, auf das für die Verwirklichung des verfolgten Ziels absolut Notwendige beschränken müssen, vgl. zuletzt Urteil Prokuratuur (Rn. 38). Der Grundsatz der Datenminimierung ist u. a. in Art. 5 Abs. 1 Buchst. c der DSGVO und Art. 4 Abs. 1 Buchst. c der Polizei-Richtlinie vorgesehen.

160 Vgl. u. a. EGMR, 18. April 2013, M. K./Frankreich (CE:ECHR:2013:0418JUD001952209, § 35).

161 Vgl. Erläuternder Bericht zum Übereinkommen Nr. 108 von 1981 (https://rm.coe.int/16800ca471), Art. 5 Nr. 40, sowie Erläuternder Bericht zum modernisierten Übereinkommen Nr. 108, Art. 5 Nr. 51.

162 Vgl. Nrn. 154 bis 158 und 162 bis 164 der vorliegenden Schlussanträge.

163 Vgl. Nrn. 133 bis 153 der vorliegenden Schlussanträge.

170. Insbesondere in Bezug auf die API-Daten, hinsichtlich derer das vorlegende Gericht vor allem Bedenken hat, stelle ich fest, dass diesen Daten, die biografischer Natur sind und die zurückgelegte Strecke betreffen, in der Regel nur wenige Informationen über das Privatleben der betreffenden Fluggäste entnommen werden können. Darüber hinaus stellt Anhang I Nr. 18 zwar auf Informationen ab, die nicht zu den in Art. 3 Abs. 2 der API-Richtlinie ausdrücklich erwähnten Informationen gehören; diese Informationen über die Identität des Fluggasts (das Geschlecht), das verwendete Reisedokument (Ausstellungsland und Ablaufdatum von Identitätsdokumenten) oder aber den gewählten Flug (Fluggesellschaft, Flugnummer, Tag sowie Flughafen des Abflugs und der Ankunft) überschneiden sich allerdings teilweise oder können PNR-Daten entnommen werden, die in anderen Nummern von Anhang I, beispielsweise den Nrn. 3, 7 und 13, aufgeführt sind. Soweit sich die Informationen auf biografische Daten oder die verwendeten Reisedokumente beziehen, können sie den Strafverfolgungsbehörden außerdem dabei helfen, die Identität einer Person zu überprüfen, und minimieren auf diese Weise, wie im neunten Erwägungsgrund der PNR-Richtlinie festgestellt wird, die Gefahr, dass ungerechtfertigte Überprüfungen und Ermittlungen zu unschuldigen Personen durchgeführt werden. Schließlich kann die bloße Tatsache, dass Anhang I Nr. 18 mehr Daten als in Art. 3 Abs. 2 der API-Richtlinie vorgesehen aufführt, nicht automatisch zu der Feststellung führen, dass diese Daten übermäßig sind, da die API-Richtlinie und die PNR-Richtlinie unterschiedliche Ziele verfolgen.

171. Die in Anhang I Nr. 12 aufgeführten Daten zu unbegleiteten Minderjährigen beziehen sich wiederum auf eine gefährdete Personengruppe, die besonderen Schutz, auch in Bezug auf die Achtung ihres Privatlebens und den Schutz ihrer personenbezogenen Daten, genießt[164]. Gleichwohl kann sich eine Einschränkung dieser Rechte als notwendig erweisen, insbesondere um Kinder vor schwerer Kriminalität, deren Opfer sie sein können, wie beispielsweise Handel mit und sexuelle Ausbeutung von Kindern oder Kindesentführung, zu schützen. Es kann somit nicht von vornherein davon ausgegangen werden, dass Anhang I Nr. 12, soweit darin die Übermittlung einer größeren Menge personenbezogener Daten zu unbegleiteten Minderjährigen vorgeschrieben ist, das absolut notwendige Maß übersteigt.

172. Auch wenn die personenbezogenen Daten, die die Fluggesellschaften den PNR-Zentralstellen gemäß der PNR-Richtlinie zu übermitteln haben, nach meinem Dafürhalten den Erfordernissen der Zweckentsprechung und der Erheblichkeit genügen und ihr Umfang das für das Funktionieren des mit dieser Richtlinie geschaffenen Systems absolut notwendige Maß nicht übersteigt, betrifft eine solche Übermittlung für jeden betroffenen Fluggast gleichwohl eine signifikante Anzahl personenbezogener Daten unterschiedlichster Art und in absoluten Werten eine extrem hohe Zahl derartiger Daten. Unter diesen Umständen ist es unbedingt erforderlich, dass die Übermittlung mit ausreichenden Garantien versehen wird, die einerseits dafür sorgen, dass nur die ausdrücklich erwähnten Daten übermittelt werden, und andererseits die Sicherheit und Vertraulichkeit der übermittelten Daten gewährleisten.

173. In diesem Zusammenhang ist zum einen zu bemerken, dass der Unionsgesetzgeber zunächst eine Reihe von Garantien vorgesehen hat, mit denen sich die Kategorien der von den Strafverfolgungsbehörden zugänglich gemachten PNR-Daten begrenzen lassen und sichergestellt werden kann, dass der Zugang auf Daten beschränkt bleibt, deren Verarbeitung als für die Verwirklichung der mit der PNR-Richtlinie verfolgten Ziele notwendig erachtet wird. So werden in dieser Richtlinie erstens – vorbehaltlich der im Rahmen der Beantwortung der dritten Vorlagefrage angestellten Erwägungen – abschließend und präzise die Daten aufgeführt, die an die PNR-Zentralstellen übermittelt werden dürfen. Zweitens wird in der PNR-Richtlinie

[164] Das Recht des Kindes auf Achtung seines Privatlebens ist u. a. in Art. 16 des am 20. November 1989 angenommenen und am 2. September 1990 in Kraft getretenen Übereinkommens von New York über die Rechte des Kindes niedergelegt.

ausdrücklich darauf hingewiesen, dass nur Daten, die in dieser sich aus einer Abwägung der im 15. Erwägungsgrund der Richtlinie erwähnten verschiedenen Interessen und Erfordernisse ergebenden Liste enthalten sind, an die PNR-Zentralstellen übermittelt werden dürfen (Art. 6 Abs. 1 der PNR-Richtlinie). Drittens werden, wenn die übermittelten PNR-Daten andere als die in Anhang I genannten Daten beinhalten, diese Daten von der PNR-Zentralstelle „unmittelbar nach ihrem Eingang dauerhaft gelöscht" (Art. 6 Abs. 1 der PNR-Richtlinie). Viertens sieht die Richtlinie vor, dass die in Anhang I aufgeführten PNR-Daten nur übermittelt werden dürfen, soweit sie von den Fluggesellschaften im Rahmen ihrer normalen Geschäftstätigkeit bereits erhoben worden sind (Art. 8 Abs. 1 und achter Erwägungsgrund der PNR-Richtlinie), was bedeutet, dass die PNR-Zentralstellen nicht automatisch auf alle in Anhang I enthaltenen Daten zugreifen können, sondern nur auf die Daten im Buchungssystem des betreffenden Wirtschaftsteilnehmers. Fünftens schreibt Art. 8 Abs. 1 der PNR-Richtlinie den Fluggesellschaften vor, bei der Übermittlung der PNR-Daten an die PNR-Zentralstellen die „Push-Methode" zu verwenden. Diese Methode, die in den ICAO-Leitlinien empfohlen wird [165], besagt, dass die Fluggesellschaften die PNR-Daten selbst an die Datenbanken der PNR-Zentralstellen übermitteln. Verglichen mit der „Pull-Methode", die es den zuständigen Behörden ermöglicht, direkt auf die Systeme der Betreiber zuzugreifen und aus deren Datenbanken eine Kopie der verlangten Daten zu extrahieren, weist die „Push-Methode" mehr Garantien auf, da sie der betreffenden Fluggesellschaft die Rolle einer Wächterin und Kontrolleurin über die PNR-Daten überträgt. Schließlich sieht die PNR-Richtlinie im Einklang mit den ICAO-Leitlinien und dem Grundsatz der „einzigen Anlaufstelle" [166] vor, dass die Übermittlung der PNR-Daten über eine einzige Einrichtung – die PNR-Zentralstelle – erfolgt, die unter der Aufsicht des in Art. 5 dieser Richtlinie genannten Datenschutzbeauftragten und vor allem unter der Aufsicht der in deren Art. 15 erwähnten nationalen Kontrollstelle tätig wird.

174. Zum anderen sieht die PNR-Richtlinie eine Reihe von Garantien vor, mit denen die *Sicherheit* der PNR-Daten gewährleistet werden soll. Ich verweise insoweit auf Art. 13 Abs. 2 dieser Richtlinie, wonach die Art. 28 und 29 der Polizei-Richtlinie, die sich auf die Vertraulichkeit der Verarbeitung und die Datensicherheit beziehen, auf jede Verarbeitung personenbezogener Daten nach der PNR-Richtlinie Anwendung finden, sowie auf Abs. 3 desselben Artikels, in dem in Bezug auf die Verarbeitung von PNR-Daten durch Fluggesellschaften auf die Pflichten hingewiesen wird, die diesen nach der DSGVO, insbesondere hinsichtlich der zum Schutz der Sicherheit und Vertraulichkeit der Daten zu treffenden geeigneten technischen und organisatorischen Maßnahmen, obliegen [167].

175. Schließlich ist hervorzuheben, dass die PNR-Richtlinie in ihren Erwägungsgründen 29 und 37 das Recht von Fluggästen anerkennt, u. a. über die Erhebung der PNR-Daten „korrekt und auf leicht zugängliche und verständliche Weise informiert" zu werden, und die Mitgliedstaaten auffordert, die Achtung dieses Rechts sicherzustellen. Auch wenn dessen Anerkennung im Text der PNR-Richtlinie nicht in einer verbindlichen Bestimmung zum Ausdruck kommt, erinnere ich daran, dass die Bestimmungen der DSGVO, wie ich bei der Prüfung der ersten Vorlagefrage ausgeführt habe, auf die Übermittlung von PNR-Daten an die

165 Vgl. Nr. 2.7.3 der ICAO-Leitlinien.

166 Vgl. Nr. 2.7.4 der ICAO-Leitlinien.

167 Das Erfordernis, die Sicherheit und Zuverlässigkeit der Datenübermittlung an die PNR-Zentralstellen zu gewährleisten, wird im Übrigen in Art. 16 Abs. 1 der PNR-Richtlinie, der sich auf die für diese Übermittlung verwendeten elektronischen Hilfsmittel bezieht, in Erinnerung gerufen und ist eines der Kriterien gewesen, an die sich die Kommission bei der in Art. 16 Abs. 3 geforderten Annahme der gemeinsamen Protokolle und Datenformate, die von den Fluggesellschaften für die Übermittlung zu verwenden sind, gehalten hat; vgl. Durchführungsbeschluss (EU) 2017/759 der Kommission vom 28. April 2017 über die gemeinsamen Protokolle und Datenformate, die von den Fluggesellschaften für die Übermittlung von Fluggastdatensätzen (PNR-Daten) an PNR-Zentralstellen zu verwenden sind (ABl. 2017, L 113, S. 48).

PNR-Zentralstellen Anwendung finden. Die Fluggesellschaften sind daher im Rahmen dieser Übermittlung verpflichtet, u. a. den Art. 13 und 14 der DSGVO nachzukommen, die das Recht auf Information von Personen vorsehen, die von einer Verarbeitung personenbezogener Daten betroffen sind. Die Mitgliedstaaten sollten das Informationsrecht von Fluggästen, wie es in den Erwägungsgründen 29 und 37 der PNR-Richtlinie anerkannt wird, im Rahmen der Umsetzung dieser Richtlinie zwar ausdrücklich vorsehen, dürfen den Anwendungsbereich der Art. 13 und 14 der DSGVO jedoch auf keinen Fall nach Art. 23 Abs. 1 dieser Verordnung beschränken, da das dem Geist der Richtlinie zuwiderliefe. Um wirksam zu sein, muss sich ein solches Recht auch auf die Kategorien von PNR-Daten beziehen, die Gegenstand einer Übermittlung sind.

176. Nach alledem vertrete ich die Ansicht, dass die PNR-Daten, deren Verarbeitung die PNR-Richtlinie vorsieht, in Anbetracht der mit dieser Richtlinie verfolgten Zwecke und vorbehaltlich der im Rahmen der dritten Vorlagefrage vorgeschlagenen Einschränkungen und vorgenommenen Klarstellungen erheblich, angemessen und nicht übermäßig sind und ihr Umfang das für die Verwirklichung dieser Zwecke absolut notwendige Maß nicht übersteigt.

– *Zu den sensiblen Daten*

177. Die PNR-Richtlinie verbietet allgemein jede Verarbeitung „sensibler Daten“ [168].

178. Auch wenn diese Richtlinie keine Definition des Begriffs „sensible Daten“ enthält, geht aus ihrem Art. 13 Abs. 4 hervor, dass sie zumindest „PNR-Daten [einschließt], die die rassische oder ethnische Herkunft einer Person, ihre politischen Meinungen, ihre religiösen oder weltanschaulichen Überzeugungen, ihre Mitgliedschaft in einer Gewerkschaft, ihren Gesundheitszustand oder ihr Sexualleben oder ihre sexuelle Orientierung erkennen lassen“ [169]. In Rn. 165 des Gutachtens 1/15 hat der Gerichtshof klargestellt, dass jede Maßnahme, die auf dem Postulat beruht, dass eines oder mehrere dieser Merkmale „als solche, unabhängig vom konkreten Verhalten des betreffenden Fluggasts, für das … Ziel der Verarbeitung von PNR-Daten erheblich sein könnte, gegen die in den Art. 7 und 8 der Charta in Verbindung mit deren Art. 21 niedergelegten Rechte verstößt“. Durch das Verbot jeder Verarbeitung der in ihrem Art. 13 Abs. 4 genannten Daten respektiert die PNR-Richtlinie somit die Grenzen, die der Gerichtshof der Verwendung dieser Datenkategorien im Rahmen eines Systems zur Verarbeitung von PNR-Daten – unabhängig davon, ob es unter das nationale Recht, das Unionsrecht oder ein von der Union abgeschlossenes internationales Übereinkommen fällt – gesetzt hat.

179. Das mit der PNR-Richtlinie aufgestellte allgemeine Verbot der Verarbeitung sensibler Daten schließt auch ihre *Erhebung* ein. Daher beruhen die in Anhang I enthaltenen 19 Rubriken, worauf im 15. Erwägungsgrund dieser Richtlinie ausdrücklich hingewiesen wird, nicht auf den in deren Art. 13 Abs. 4 genannten PNR-Daten.

180. Auch wenn keine der Rubriken ausdrücklich auf solche Daten abstellt, könnten diese gleichwohl u. a. unter die in Anhang I Nr. 12 aufgeführte Rubrik „Allgemeine Hinweise“ fallen, bei der es sich um ein „offenes Feld“ handelt, das, wie ich im Rahmen der Prüfung der dritten Vorlagefrage bereits festgestellt habe, eine unbestimmte Zahl von Informationen unterschiedlichster Art umfassen kann. Es besteht nämlich, wie der Gerichtshof im Übrigen in Rn. 164 des Gutachtens 1/15 bemerkt hat, eine konkrete Gefahr, dass aus Informationen, die

168 Vgl. 37. Erwägungsgrund der PNR-Richtlinie.

169 Die in Art. 13 Abs. 4 der PNR-Richtlinie aufgeführten Kategorien personenbezogener Daten sind allesamt in den Kategorien enthalten, die dem Begriff „besondere Kategorien personenbezogener Daten“ in Art. 9 Abs. 1 der DSGVO entsprechen.

unter die besagte Rubrik fallen und sich beispielsweise auf Ernährungsgewohnheiten, Unterstützungsanfragen, Preispauschalen zugunsten bestimmter Personengruppen oder Kategorien von Organisationen beziehen, unmittelbar sensible Daten im Sinne von Art. 13 Abs. 4 der PNR-Richtlinie u. a. zu den religiösen Überzeugungen der betreffenden Fluggäste, ihrem Gesundheitszustand oder ihrer Mitgliedschaft in einer Gewerkschaft oder einer politischen Partei hervorgehen.

181. Da diese Daten nach der PNR-Richtlinie keinesfalls verarbeitet werden dürfen, übersteigt ihre Übermittlung durch die Fluggesellschaften nicht nur offensichtlich das absolut notwendige Maß, sondern hat auch keinerlei Nutzen. Der Tatsache, dass die PNR-Zentralstellen gemäß Art. 13 Abs. 4 Satz 2 der PNR-Richtlinie in jedem Fall verpflichtet sind, PNR-Daten, aus denen eine der in Satz 1 dieses Absatzes aufgezählten Informationen hervorgeht, umgehend zu löschen, lässt sich insoweit nicht entnehmen, dass eine Datenübermittlung gestattet oder gerechtfertigt wäre [170], weil das mit der Richtlinie aufgestellte Verarbeitungsverbot ab dem ersten Schritt der Verarbeitung von PNR-Daten greifen soll. Die Verpflichtung zur Löschung sensibler Daten stellt somit nur eine zusätzliche Garantie dar, die diese Richtlinie für den Fall vorsieht, dass solche Daten ausnahmsweise irrtümlich an die PNR-Zentralstellen übermittelt werden.

182. Da Informationen, die unter „free text"-Rubriken wie beispielsweise die Rubrik „Allgemeine Hinweise" in Anhang I Nr. 12 fallen, in denen sensible Daten gemäß Art. 13 Abs. 4 der PNR-Richtlinie enthalten sein könnten, von den Fluggästen nur fakultativ mitgeteilt werden, ist es, wie Generalanwalt Mengozzi in Nr. 222 seiner Schlussanträge im Gutachten 1/15 [171] bemerkt hat, darüber hinaus wenig wahrscheinlich, dass Personen, die an terroristischen oder der schweren Kriminalität zuzuordnenden Straftaten beteiligt sind, eine solche spontane Mitteilung vornehmen, so dass die systematische Übermittlung dieser Daten zumeist nur Personen betreffen dürfte, die eine zusätzliche Leistung verlangt haben und tatsächlich von keinerlei Interesse für die Strafverfolgungsbehörden sind [172].

183. Im Rahmen der Prüfung der dritten Vorlagefrage bin ich zu dem Schluss gelangt, dass Anhang I Nr. 12 in Bezug auf die Rubrik „Allgemeine Hinweise" den sich aus Art. 52 Abs. 1 Satz 1 der Charta ergebenden Erfordernissen der Klarheit und Präzision nicht genügt. Aus den soeben dargelegten Gründen bin ich der Ansicht, dass die Aufnahme dieser Rubrik in die Kategorien von Daten, die systematisch an die PNR-Zentralstellen übermittelt werden, ohne dass eine Klarstellung hinsichtlich der Informationen erfolgt, auf die sie sich beziehen kann, ebenso wenig dem in Art. 52 Abs. 1 Satz 2 der Charta vorgesehenen Kriterium der Erforderlichkeit in der Auslegung durch den Gerichtshof genügt [173].

184. Abgesehen davon reicht es nicht aus, die sogenannten „free text"-Rubriken von der Liste der den staatlichen Behörden im Rahmen eines Systems zur Verarbeitung von PNR-Daten zu übermittelnden PNR-Daten zu entfernen, um die Gefahr zu bannen, dass sensible Daten diesen Behörden gleichwohl zur Verfügung gestellt werden. Solche Daten lassen sich nämlich nicht nur

[170] Das Vorbringen mehrerer Mitgliedstaaten, die Erklärungen zur zweiten Vorlagefrage abgegeben haben, wonach es technische Hilfsmittel gebe, mit denen sich von den Fluggesellschaften übermittelte sensible Daten leicht löschen ließen, ist nach meinem Dafürhalten in diesem Zusammenhang irrelevant.

[171] Schlussanträge des Generalanwalts Mengozzi im Gutachten 1/15 (PNR-Abkommen EU–Kanada), EU:C:2016:656.

[172] Sogar die ICAO-Leitlinien schließen nicht aus, dass sensible Daten, die sich den „free text"-Rubriken entnehmen lassen, für die Bewertung der Gefahr, die von einem Fluggast ausgehen kann, möglicherweise von Nutzen sind, empfehlen den Vertragsstaaten aber gleichwohl, sicherzustellen, dass sie nur berücksichtigt werden, wenn es konkrete Anhaltspunkte gibt, die ihre Verwendung zu den mit den PNR-Systemen der Vertragsstaaten verfolgten Zwecken geboten erscheinen lassen.

[173] Ich erinnere daran, dass schon der EDSB in seiner Stellungnahme vom 25. März 2011 (Nr. 47) einen solchen Ausschluss vorgeschlagen hatte.

unmittelbar aus Informationen ableiten, die unter derartige Rubriken fallen, sondern können auch mittelbar aus Informationen hervorgehen oder aufgrund von Informationen vermutet werden, die in „verschlüsselten" Rubriken enthalten sind. So kann der Name des Fluggasts, um ein Beispiel zu geben, Hinweise auf die ethnische Herkunft oder die Religionszugehörigkeit des betreffenden Fluggasts liefern oder zumindest zur Aufstellung von Hypothesen einladen. Gleiches gilt für die Staatsangehörigkeit. Diese Daten eignen sich grundsätzlich weder dazu, von der Liste der zu übermittelnden PNR-Daten entfernt zu werden, noch dazu, von den empfangsberechtigten Behörden gelöscht zu werden. Um der Gefahr vorzubeugen, dass zahlreiche Personen, die jedoch keiner Straftat verdächtig sind, auf der Grundlage geschützter Merkmale stigmatisiert werden, ist es daher wichtig, dass ein System zur Verarbeitung von PNR-Daten ausreichende Garantien vorhält, mit denen sich auf jeder Stufe der Verarbeitung der erhobenen Daten ausschließen lässt, dass solche Merkmale direkt oder indirekt berücksichtigt werden können, beispielsweise indem bei der automatisierten Analyse Selektoren angewandt werden, die auf diesen Merkmalen beruhen. Darauf werde ich im weiteren Verlauf meiner Prüfung zurückkommen.

185. Nach alledem vertrete ich vorbehaltlich der Schlussfolgerung, zu der ich oben in Nr. 183 gelangt bin, die Ansicht, dass die PNR-Richtlinie im Stadium der Übermittlung der PNR-Daten an die PNR-Zentralstellen ausreichende Garantien zum Schutz sensibler Daten vorsieht.

iii) Zum Begriff „Fluggast" (vierte Vorlagefrage)

186. Mit seiner vierten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof erfahren, ob das mit der PNR-Richtlinie geschaffene System, insofern es die allgemeine Übermittlung und Verarbeitung von PNR-Daten jeder Person, die dem Begriff „Fluggast" im Sinne von Art. 3 Nr. 4 dieser Richtlinie entspricht, unabhängig von einem objektiven Anhaltspunkt für die Annahme gestattet, dass von der betreffenden Person eine Gefahr für die öffentliche Sicherheit ausgehen könnte, mit den Art. 7, 8 und 52 Abs. 1 der Charta vereinbar ist. Es fragt sich insbesondere, ob die Rechtsprechung des Gerichtshofs im Bereich der Vorratsspeicherung und des Zugangs zu Daten in der elektronischen Kommunikation auf das mit der PNR-Richtlinie eingeführte System zur Verarbeitung personenbezogener Daten übertragen werden kann.

187. In dieser Rechtsprechung hat der Gerichtshof, soweit für das vorliegende Verfahren von Belang, festgestellt, dass eine Regelung, die zur Bekämpfung schwerer Kriminalität für den Zugang der Strafverfolgungsbehörden eine allgemeine und unterschiedslose *Vorratsspeicherung* von Verkehrsdaten zu elektronischen Kommunikationen und von Standortdaten[174] vorsieht, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels, grundsätzlich nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden kann[175]. Der Gerichtshof hat Gleiches in Bezug auf eine nationale Regelung entschieden, die zur Bekämpfung des Terrorismus eine *automatisierte Analyse aller Verkehrs- und Standortdaten* mittels einer von den Betreibern elektronischer Kommunikationsdienste auf Ersuchen der zuständigen nationalen Behörden in Anwendung der von diesen festgelegten Parametern vorgenommenen Filterung vorsah[176]. Nach Auffassung des Gerichtshofs können solche Maßnahmen nur gerechtfertigt sein, wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit

174 Hierbei handelt es sich um Daten, die Informationen über die von einem Nutzer eines elektronischen Kommunikationsmittels getätigten Mitteilungen oder über den Standort der von ihm verwendeten Endgeräte liefern könnten.

175 Vgl. in diesem Sinne Urteile La Quadrature du Net (Rn. 141 bis 145) und Tele2 Sverige (Rn. 105 und 106), die im Rahmen einer Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und 52 Abs. 1 der Charta ergangen sind, sowie Urteil Digital Rights (Rn. 57 und 58), in dem der Gerichtshof die Richtlinie 2006/24 für ungültig erklärt hat.

176 Vgl. Urteil La Quadrature du Net (Rn. 177).

gegenübersieht und die Entscheidung, die ihre Umsetzung vorsieht, Gegenstand einer wirksamen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle ist [177]. Der Rückgriff auf diese Maßnahmen in solchen Situationen muss nach Ansicht des Gerichtshofs außerdem in zeitlicher Hinsicht auf das absolut Notwendige beschränkt werden und darf jedenfalls keinen systematischen Charakter haben [178].

188. Darüber hinaus ist der Gerichtshof in der vorstehend angeführten Rechtsprechung zwar nicht so weit gegangen, das Vorliegen einer Beeinträchtigung des Wesensgehalts des Rechts auf Achtung des Privatlebens wie im Urteil Schrems I ausdrücklich festzustellen, hat aber gleichwohl die Auffassung vertreten, dass die in Rede stehenden Maßnahmen mit einem so schwerwiegenden Eingriff verbunden waren, dass sie – außer im seltenen Fall spezifischer Bedrohungen der nationalen Sicherheit eines Mitgliedstaats – schlicht und ergreifend nicht als auf das absolut Notwendige beschränkt und damit im Einklang mit der Charta stehend angesehen werden konnten [179], unabhängig von den etwaigen gegen Missbrauchsrisiken und rechtswidrigen Zugang zu den betreffenden Daten vorgesehenen Garantien [180].

189. Ich habe bereits hervorgehoben, dass eine Regelung wie die in der PNR-Richtlinie vorgesehene mit den Maßnahmen von der Art derjenigen, die der Gerichtshof in der in den vorstehenden Nummern der vorliegenden Schlussanträge in Erinnerung gerufenen Rechtsprechung untersucht hat, eine Reihe gemeinsamer Elemente teilt, die ihr einen besonders einschneidenden Charakter verleihen. So wird mit dieser Richtlinie ein allgemeines und unterschiedsloses System zur Erhebung und automatisierten Analyse der personenbezogenen Daten eines erheblichen Teils der Bevölkerung eingeführt, das pauschal für sämtliche Personen, die dem Begriff „Fluggast“ in Art. 3 Nr. 4 der Richtlinie entsprechen, und damit auch für Personen gilt, bei denen keinerlei Anhaltspunkt dafür vorliegt, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit terroristischen oder der schweren Kriminalität zuzuordnenden Aktivitäten stehen könnte. Daher stellt sich das vorlegende Gericht die Frage, ob diese Rechtsprechung auf ein System zur Verarbeitung von PNR-Daten wie das mit der PNR-Richtlinie geschaffene übertragen werden kann.

190. Bei der Prüfung des persönlichen Anwendungsbereichs des Entwurfs eines PNR-Abkommens Kanada–EU in den Rn. 186 bis 189 des Gutachtens 1/15 hat es der Gerichtshof insoweit vermieden, eine Parallele zwischen Maßnahmen zur Vorratsspeicherung sowie zum allgemeinen und unterschiedslosen Zugang zum Inhalt elektronischer Kommunikationen, zu Verkehrs- und zu Standortdaten einerseits und der Übermittlung von PNR-Daten und ihrer automatisierten Verarbeitung im Rahmen einer Vorabüberprüfung von Fluggästen, um die es in diesem Abkommen geht, andererseits, zu ziehen. Zum Zeitpunkt der Erstellung des Gutachtens gab es jedoch bereits eine gefestigte – nur wenige Monate zuvor durch das vom vorlegenden Gericht in Bezug genommene Urteil Tele2 Sverige bestätigte – Rechtsprechung, in der die besagten Maßnahmen – außer in spezifischen und vereinzelten

177 Vgl. Urteil La Quadrature du Net (Rn. 134 bis 139 und 177). Nach Ansicht des Gerichtshofs entspricht die Verantwortung, die den Mitgliedstaaten auf dem Gebiet der nationalen Sicherheit obliegt, „dem zentralen Anliegen, die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen, und umfasst die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen, wie insbesondere terroristische Aktivitäten“; vgl. Urteile La Quadrature du Net (Rn. 135) und Privacy International (Rn. 74).

178 Vgl. Urteil La Quadrature du Net (Rn. 138 und 178).

179 Vgl. u. a. Urteil La Quadrature du Net (Rn. 141 bis 145).

180 Vgl. Urteil La Quadrature du Net (Rn. 115 und 116); vgl. auch Schlussanträge des Generalanwalts Campos Sánchez-Bordona in den verbundenen Rechtssachen SpaceNet und Telekom Deutschland (C-793/19 und C-794/19, EU:C:2021:939, Nrn. 74 und 75).

Fällen [181] – für mit der Charta unvereinbar angesehen wurden [182]. Die jüngsten einschlägigen Urteile des Gerichtshofs, insbesondere das Urteil La Quadrature du Net, bewegen sich auf der Linie dieser Rechtsprechung, präzisieren sie und nuancieren sie unter bestimmten Gesichtspunkten.

191. In den genannten Randnummern des Gutachtens 1/15 hat der Gerichtshof ausdrücklich die Auffassung vertreten, dass das PNR-Abkommen Kanada–EU nicht über die Grenzen des absolut Notwendigen hinausgeht, soweit es zwecks Vorabüberprüfung die *Übermittlung* der PNR-Daten sämtlicher Fluggäste an Kanada und die *automatisierte Verarbeitung* dieser Daten gestattet, obwohl eine solche Übermittlung und eine solche Verarbeitung „unabhängig davon [erfolgen sollen], ob objektive Anhaltspunkte dafür vorliegen, dass von den Fluggästen eine Gefahr für die öffentliche Sicherheit in Kanada ausgeht“ [183]. In Rn. 187 des Gutachtens ist der Gerichtshof so weit gegangen, festzustellen, dass „[d]er Ausschluss bestimmter Kategorien von Personen oder bestimmter Herkunftsländer … dem Ziel der automatisierten Verarbeitung der PNR-Daten zuwiderlaufen [könnte], das darin besteht, unter sämtlichen Fluggästen mittels einer Überprüfung dieser Daten die Personen zu ermitteln, von denen eine Gefahr für die öffentliche Sicherheit ausgehen kann“, und dadurch „diese Überprüfung umgangen werden [könnte]“ [184].

192. Daher hat sich der Gerichtshof zumindest in Bezug auf die allgemeine und unterschiedslose Übermittlung von PNR-Daten von dem strengeren Ansatz gelöst, der im Bereich der Vorratsspeicherung und des Zugangs zu Metadaten gewählt worden war.

193. Auch wenn er in seiner Argumentation, wie u. a. aus den Rn. 152 und 188 des Gutachtens 1/15 hervorgeht, die Feststellung, wonach die automatisierte Verarbeitung von PNR-Daten die Sicherheitskontrollen, insbesondere an den Grenzen, erleichtert, einerseits, und die Tatsache, dass Fluggäste, die in das Hoheitsgebiet eines Vertragsstaats des Abkommens von Chicago einreisen möchten, nach dem Abkommen verpflichtet sind, sich den Kontrollen zu unterziehen und die Voraussetzungen dieses Staates für die Ein- oder Ausreise, einschließlich der Überprüfung ihrer PNR-Daten, zu erfüllen, unbestreitbar berücksichtigt hat, sprechen meiner Ansicht nach andere Gründe, darunter erstens die Art der verarbeiteten Daten, für unterschiedliche Ansätze.

194. Der Gerichtshof hat mehrmals betont, dass nicht nur der Inhalt der elektronischen Kommunikationen, sondern auch die Metadaten Informationen „über eine Vielzahl von Aspekten des Privatlebens der Betroffenen“ enthalten können, „einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand“, dass aus der Gesamtheit dieser Daten „sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden [können], etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren“, und dass die Daten die Erstellung „eines Profils der Betroffenen [ermöglichen], das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible

181 Vgl. Urteil Tele2 Sverige (Rn. 119).

182 Vgl. in diesem Sinne Urteil Tele2 Sverige (Rn. 103 bis 107 und 119 sowie die dort angeführte Rechtsprechung).

183 Vgl. Gutachten 1/15 (Rn. 186 und 187).

184 Sowohl in den Urteilen Digital Rights (Rn. 59) und Tele2 Sverige (Rn. 111) als auch in der späteren Rechtsprechung (vgl. u. a. Urteil La Quadrature du Net, Rn. 143 bis 150), war die in Rede stehende Regelung gerade deshalb unverhältnismäßig, weil sie nicht auf „objektiven Kriterien“ von der Art der vom Gerichtshof in Rn. 187 des Gutachtens 1/15 erwähnten Kriterien beruhte, mit denen sich eine Zielgruppe erfassen ließ, deren Daten zumindest einen mittelbaren Zusammenhang mit schweren Straftaten offenbaren konnten.

Information darstellt wie der Inhalt der Kommunikationen selbst“ [185]. Darüber hinaus sahen die bisher vom Gerichtshof untersuchten Regelungen, einschließlich der in der Richtlinie 2006/24 enthaltenen Regelung, keinerlei Ausnahme vor und galten auch für Mitteilungen an oder von Diensten sozialen oder religiösen Charakters oder von Fachleuten, die Verpflichtungen zur Wahrung des Berufsgeheimnisses unterlagen. Daher hat der Gerichtshof zwar keine Verletzung des Wesensgehalts des Rechts auf Achtung des Privatlebens festgestellt, gleichwohl aber für Recht erkannt, dass „[a]ngesichts des sensiblen Charakters der Informationen, die sich aus den Verkehrs- und Standortdaten ergeben können, … deren Vertraulichkeit … von entscheidender Bedeutung für das Recht auf Achtung des Privatlebens [ist]“ [186].

195. Dagegen hat der Gerichtshof, worauf ich in den Nrn. 77 und 98 der vorliegenden Schlussanträge hingewiesen habe, im Gutachten 1/15 zwar anerkannt, dass die PNR-Daten unter Umständen sehr genaue Informationen über das Privatleben einer Person liefern können [187], gleichwohl aber festgestellt, dass die Art dieser Informationen auf bestimmte Aspekte dieses Privatlebens beschränkt ist [188], was den Zugang zu solchen Daten weniger einschneidend macht als den Zugang zum Inhalt der elektronischen Kommunikationen sowie zu den Verkehrs- und Standortdaten.

196. Zweitens unterscheiden sich PNR-Daten nicht nur hinsichtlich ihrer Art von Verkehrs- und Standortdaten; auch die Anzahl und die Vielfalt der Informationen, die aus diesen unterschiedlichen Datenkategorien hervorgehen könnten, unterscheiden sich, da in PNR-Daten sowohl in quantitativer als auch in qualitativer Hinsicht weniger Informationen enthalten sind. Dies hängt nicht nur von der Tatsache, dass Systeme zur allgemeinen und unterschiedslosen Verarbeitung von Daten zu elektronischen Kommunikationen fast die gesamte Zielbevölkerung betreffen können, während Systeme zur Verarbeitung von PNR-Daten für einen begrenzteren, wenn auch zahlenmäßig bedeutenden Personenkreis gelten, sondern auch von der Häufigkeit der Nutzung und der Vielzahl der elektronischen Kommunikationsmittel ab. Darüber hinaus sieht die PNR-Richtlinie die Erhebung und Verarbeitung einer begrenzten und erschöpfend festgelegten Anzahl von PNR-Daten unter Ausschluss von Daten vor, die unter die in Art. 13 Abs. 4 dieser Richtlinie aufgeführten Kategorien fallen, so dass sich wenn nicht die Menge, so zumindest die Sensibilität der Informationen über das Privatleben der betreffenden Personen, die sich daraus ergeben können, teilweise im Voraus beurteilen lässt [189]. Eine solche Begrenzung der Typologie von Zieldaten, mit der sich ein großer Teil der Daten ausschließen lässt, die sensible Informationen enthalten könnten, ist unter Berücksichtigung der Anzahl von Nutzern und betroffenen Kommunikationsmitteln bei Verkehrs- und Standortdaten jedoch nur zum Teil möglich [190].

197. Drittens ist jede Verarbeitung von Metadaten elektronischer Kommunikationen nicht nur geeignet, die Intimsphäre des Lebens nahezu der gesamten Bevölkerung zu berühren, sondern beeinträchtigt auch die Ausübung anderer Freiheiten, durch die der Einzelne am sozialen und demokratischen Leben eines Landes teilhat [191], und droht insbesondere eine abschreckende Wirkung auf die Freiheit der Meinungsäußerung der Nutzer elektronischer

185 Vgl. Urteil La Quadrature du Net (Rn. 117 und die dort angeführte Rechtsprechung); vgl. auch Urteil Prokuratuur (Rn. 36).

186 Urteil La Quadrature du Net (Rn. 142).

187 Vgl. Gutachten 1/15 (Rn. 128 und 150).

188 Vgl. Gutachten 1/15 (Rn. 150).

189 Zur Schwierigkeit einer solchen Beurteilung in Bezug auf Metadaten vgl. Urteil Prokuratuur (Rn. 40).

190 Anstrengungen in diese Richtung hat der deutsche Gesetzgeber in der Regelung unternommen, die Gegenstand der verbundenen Rechtssachen C-793/19 und C-794/19, SpaceNet und Telekom Deutschland, ist, in denen Generalanwalt Campos Sánchez-Bordona seine Schlussanträge vorgelegt hat (EU:C:2021:939, Nrn. 60 und 61).

191 Ich verweise insoweit auf Nr. 93 der vorliegenden Schlussanträge.

Kommunikationsmittel zu haben [192], die „eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft“ darstellt, welche zu den Werten gehört, auf die sich die Union gründet [193]. Dieser Aspekt ist den Maßnahmen für die genannten Kategorien personenbezogener Daten inhärent und betrifft Systeme zur Verarbeitung von PNR-Daten grundsätzlich nicht.

198. Viertens besteht – hauptsächlich aufgrund der Anzahl und Vielfalt der sensiblen Informationen, die dem Inhalt der elektronischen Kommunikationen sowie den Verkehrs- und Standortdaten entnommen werden können – ein signifikant höheres Risiko von Willkür im Zusammenhang mit der Verarbeitung dieser Daten als bei Systemen zur Verarbeitung von PNR-Daten.

199. Vor diesem Hintergrund bin ich der Ansicht, dass der vom Gerichtshof im Bereich der elektronischen Kommunikation gewählte strengere Ansatz als solcher nicht auf Systeme zur Verarbeitung von PNR-Daten übertragbar ist. Im Gutachten 1/15 hat sich der Gerichtshof im Kontext eines internationalen Übereinkommens über die Einführung eines solchen Systems zum Schutz der Sicherheit eines Drittlandes bereits – zumindest implizit – in diesem Sinne geäußert. Die gleiche Position ist nach meinem Dafürhalten erst recht in Bezug auf die PNR-Richtlinie gerechtfertigt, deren Ziel der Schutz der inneren Sicherheit der Union ist.

200. Abgesehen davon ist zu bemerken, wie es Generalanwalt Mengozzi in Nr. 216 seiner Schlussanträge im Gutachten 1/15 getan hat [194], dass die Bedeutung der Systeme zur Verarbeitung von PNR-Daten, seien sie einseitig erlassen oder Gegenstand eines internationalen Abkommens, gerade in der Garantie der massenhaften Übermittlung von Daten liegt, die den zuständigen Behörden erlaubt, mit Hilfe von Instrumenten zur automatisierten Verarbeitung und im Voraus festgelegten Szenarien oder Beurteilungskriterien Personen zu identifizieren, die den Strafverfolgungsbehörden unbekannt waren, aber für die öffentliche Sicherheit von „Interesse“ oder eine Gefahr sein könnten und daher später eingehenderen individuellen Kontrollen unterzogen werden können. Das in der Rechtsprechung des EGMR zu zielgerichteten Überwachungen im Rahmen strafrechtlicher Ermittlungen [195] und in der Rechtsprechung des Gerichtshofs zur Vorratsspeicherung von Metadaten [196] aufgestellte Erfordernis eines „begründeten Verdachts“ ist im Kontext einer solchen Übermittlung und Verarbeitung daher weniger relevant [197]. Auch insbesondere das mit solchen Systemen verfolgte Präventionsziel lässt sich nicht erreichen, wenn die Anwendung der Systeme auf eine bestimmte Personengruppe beschränkt wird, wie der Gerichtshof im Übrigen in den in Nr. 191 der vorliegenden Schlussanträge wiedergegebenen Randnummern des Gutachtens 1/15 festgestellt hat, so dass der Geltungsbereich der PNR-Richtlinie die wirksame Erreichung dieses Ziels zu gewährleisten scheint [198].

201. Darüber hinaus ist hervorzuheben, dass die Kommission die strategische Bedeutung der Verarbeitung von PNR-Daten als wesentliches Instrument der gemeinsamen Reaktion der Union auf Terrorismus und schwere Kriminalität und als wichtiger Bestandteil der Sicherheitsunion

192 Vgl. Urteil La Quadrature du Net (Rn. 118 und die dort angeführte Rechtsprechung).

193 Vgl. Urteil Tele2 Sverige (Rn. 93).

194 Schlussanträge des Generalanwalts Mengozzi im Gutachten 1/15 ([PNR-Abkommen EU–Kanada], EU:C:2016:656).

195 Vgl. u. a. EGMR, 4. Dezember 2015, Roman Zakharov/Russland (CE:ECHR:2015:1204JUD004714306, § 260).

196 Vgl. Urteile La Quadrature du Net (Rn. 146 bis 151) und Tele2 Sverige (Rn. 119).

197 Vgl. in diesem Sinne – zu Massenüberwachungsmaßnahmen – Urteil Big Brother Watch (§ 348).

198 Vgl. entsprechend Urteil vom 3. Oktober 2019, A u. a. (C-70/18, EU:C:2019:823, Rn. 61).

mehrfach herausgestellt hat[199]. Im Rahmen eines „umfassenden Ansatzes“ zur Bekämpfung des Terrorismus ist die Rolle der Systeme zur Verarbeitung von PNR-Daten auch vom Sicherheitsrat der Vereinten Nationen anerkannt worden, der die Mitgliedstaaten der Vereinten Nationen in der Resolution 2396 (2017)[200] dazu verpflichtet hat, „zur Durchführung der Richtlinien und Empfehlungen der ICAO Kapazitäten zur Sammlung, Verarbeitung und Analyse von [PNR-]Daten auf[zu]bauen und dafür [zu] sorgen …, dass alle ihre zuständigen nationalen Behörden diese Daten unter voller Achtung der Menschenrechte und Grundfreiheiten nutzen und weitergeben, um terroristische Straftaten und damit zusammenhängende Reisen von Terroristen zu verhüten, aufzudecken und zu untersuchen“[201]. Diese Verpflichtung wird in der Resolution 2482/2019 auf dem Gebiet des Terrorismus und schwerer grenzübergreifender Kriminalität[202] bekräftigt.

202. In diesem Kontext erlaubt es die Verabschiedung eines auf Unionsebene harmonisierten Systems zur Verarbeitung von PNR-Daten sowohl in Bezug auf Drittstaatsflüge als auch – für Staaten, die von Art. 2 der PNR-Richtlinie Gebrauch gemacht haben – in Bezug auf EU-Flüge, zu gewährleisten, dass die Verarbeitung dieser Daten unter Wahrung des in der Richtlinie festgelegten hohen Schutzniveaus für die in den Art. 7 und 8 der Charta niedergelegten Rechte erfolgt, und stellt ein Referenzrechtssystem für die Aushandlung internationaler Übereinkommen über die Verarbeitung und Übermittlung von PNR-Daten bereit[203].

203. Wenn es zutrifft, dass das mit der PNR-Richtlinie geschaffene System unterschiedslos alle Fluggäste erfasst, wie u. a. das Parlament in seinen schriftlichen Erklärungen zu Recht unterstrichen und auch der Sicherheitsrat der Vereinten Nationen in der Resolution 2396 (2017), in der auf die konkrete Gefahr einer Verwendung der zivilen Luftfahrt zu terroristischen Zwecken sowohl als Beförderungsmittel als auch als Ziel hingewiesen wird, herausgestellt hat[204], besteht darüber hinaus u. a. beim Terrorismus und zumindest bei bestimmten Formen schwerer Kriminalität wie insbesondere dem Drogen- oder Menschenhandel, die im Übrigen eine starke grenzüberschreitende Komponente aufweisen, ein objektiver Zusammenhang zwischen Luftverkehr und Bedrohungen für die öffentliche Sicherheit.

204. Schließlich ist hervorzuheben, dass, wie das Parlament, der Rat und mehrere Mitgliedstaaten, die schriftliche Erklärungen eingereicht haben, geltend gemacht haben, Fluggäste bei Einreise in die oder Ausreise aus der Union verpflichtet sind, sich

199 Vgl. unlängst Mitteilung der Kommission – EU-Strategie für eine Sicherheitsunion (KOM[2020] 605 endg., S. 28) sowie Mitteilung der Kommission – Eine EU-Agenda für Terrorismusbekämpfung: antizipieren, verhindern, schützen und reagieren (KOM[2020] 795 endg., S. 15 f.).

200 Resolution vom 21. Dezember 2017 (im Folgenden: Resolution 2396 [2017]), https://undocs.org/fr/S/RES/2396(2017).

201 Vgl. Resolution 2396 (2017), Nr. 12; in derselben Nr. 12 fordert der VN-Sicherheitsrat „die ICAO nachdrücklich [auf], in Zusammenarbeit mit den Vertragsstaaten eine Richtlinie zur Sammlung, Nutzung und Verarbeitung von Daten aus Fluggastdatensätzen und zum Schutz dieser Daten festzulegen“. Infolge dieser Aufforderung hat die ICAO am 23. Juni 2020 die Änderung 28 zu Anhang 9 des Abkommens von Chicago angenommen, der, wie bereits ausgeführt worden ist, internationale Richtlinien zur „Erleichterung“ enthält und dessen Kapitel 9 Abschnitt D sich speziell auf Fluggastdatensätze bezieht. Am 12. Januar 2021 hat die Kommission einen Vorschlag für einen Beschluss des Rates über den Standpunkt angenommen, der im Namen der Europäischen Union in der [ICAO] bezüglich dieser Änderung zu vertreten ist (KOM[2021] 16 endg.).

202 Resolution vom 19. Juli 2019, Nr. 15(c), https://undocs.org/fr/S/RES/2482(2019).

203 Zum gegenwärtigen Zeitpunkt hat die Union zwei internationale Abkommen mit Australien (Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von [PNR-Daten] und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service [ABl. 2012, L 186, S. 4]) bzw. den Vereinigten Staaten von Amerika (Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von [PNR-Daten] und deren Übermittlung an das United States Department of Homeland Security [ABl. 2012, L 215, S. 5]) abgeschlossen. Eine gemeinsame Bewertung dieser beiden Abkommen im Hinblick auf den Abschluss weiterer Abkommen ist im Gang. Am 18. Februar 2020 hat der Rat der Kommission außerdem ein Mandat für die Aufnahme von Verhandlungen mit Japan erteilt.

204 Vgl. Resolution 2396 (2017), S. 4.

Sicherheitskontrollen zu unterziehen [205]. Die Übermittlung und Verarbeitung der PNR-Daten vor ihrer Ankunft oder Abreise erleichtert und beschleunigt diese Kontrollen, wie auch der Gerichtshof im Gutachten 1/15 festgestellt hat, und ermöglicht es den Strafverfolgungsbehörden, sich auf jene Fluggäste zu konzentrieren, bei denen konkret angenommen wird, dass sie ein Sicherheitsrisiko darstellen könnten [206].

205. Was abschließend insbesondere die Ausweitung des Systems der PNR-Richtlinie auf EU-Flüge angeht, so ist, auch wenn sich Auswirkungen auf die u. a. in Art. 45 der Charta verankerte Freizügigkeit der Unionsbürger nicht von vornherein ausschließen lassen, der mit der PNR-Richtlinie verbundene Eingriff in das Privatleben zwar schwer, hat nach meinem Dafürhalten als solcher aber keine abschreckende Wirkung auf die Ausübung dieser Freiheit, da die Verarbeitung von PNR-Daten von der Öffentlichkeit sogar als eine für die Gewährleistung der Sicherheit des Luftverkehrs notwendige Maßnahme wahrgenommen werden kann [207]. Das ändert nichts daran, dass fortlaufend bewertet und überwacht werden muss, ob eine solche abschreckende Wirkung vorliegt.

206. Um der in den Nrn. 107 und 108 der vorliegenden Schlussanträge wiedergegebenen Rechtsprechung Rechnung zu tragen, darf sich die PNR-Richtlinie jedoch nicht darauf beschränken, dass der Zugang zu den PNR-Daten sämtlicher Fluggäste und die automatisierte Verarbeitung dieser Daten dem verfolgten Zweck zu entsprechen haben, sondern muss auch klar und präzise die materiellen und prozeduralen Voraussetzungen für diesen Zugang und diese Verarbeitung sowie für die spätere Verwendung der Daten vorsehen [208] und in jeder Phase dieses Prozesses angemessene Garantien bereitstellen. Ich habe die Garantien, mit denen die Übermittlung der PNR-Daten an die PNR-Zentralstellen versehen ist, bei der Prüfung der zweiten Vorlagefrage bereits genannt. Anlässlich der Prüfung der sechsten Vorlagefrage werde ich einen Überblick über die Garantien, die speziell mit der automatisierten Verarbeitung dieser Daten einhergehen, und im Rahmen der Prüfung der achten Vorlagefrage über diejenigen geben, die mit deren Vorratsspeicherung zusammenhängen.

207. Bevor ich mit der Prüfung fortfahre, möchte ich die grundlegende Bedeutung unterstreichen, die der Kontrolle durch die in Art. 15 der PNR-Richtlinie genannte unabhängige Stelle im Rahmen des mit dieser Richtlinie geschaffenen Garantiesystems zukommt. Danach unterliegt jede Datenverarbeitung gemäß der Richtlinie der Kontrolle durch eine unabhängige Kontrollstelle, die befugt ist, die Rechtmäßigkeit dieser Verarbeitung zu prüfen, Ermittlungen, Inspektionen und Audits durchzuführen sowie Beschwerden betroffener Personen zu behandeln. Eine solche Kontrolle durch eine externe Stelle, die für die Verteidigung von Interessen zuständig ist, die mit den Interessen der Verarbeiter von PNR-Daten in Konflikt geraten könnten, und der die Rolle zufällt, die Einhaltung sämtlicher Einschränkungen und Schutzvorkehrungen im Zusammenhang mit diesen Verarbeitungen zu gewährleisten, stellt eine in Art. 8 Abs. 3 der Charta ausdrücklich genannte wesentliche Garantie dar, die in Bezug auf den Schutz der betroffenen Grundrechte sogar eine höhere Wirksamkeit hat als das System der Rechtsbehelfe, die Einzelpersonen zur Verfügung stehen. Nach meinem Dafürhalten ist es daher von grundlegender Bedeutung, dass der Gerichtshof den Umfang der in Art. 15 der PNR-Richtlinie vorgesehenen Kontrollbefugnisse weit auslegt und die Mitgliedstaaten ihrer nationalen

[205] Einschließlich Personen, die nach Unionsrecht Anspruch auf freien Personenverkehr haben; vgl. Verordnung (EU) 2017/458 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Änderung der Verordnung (EU) 2016/399 hinsichtlich einer verstärkten Abfrage von einschlägigen Datenbanken an den Außengrenzen (ABl. 2017, L 74, S. 7).

[206] Vgl. in diesem Sinne auch Gutachten 1/15 (Rn. 187). Vgl. auch Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer (KOM[2010] 492 endg., S. 6, Nr. 2.2).

[207] Das ist gewissermaßen das, was die Kommission in ihrem Vorschlag für eine PNR-Richtlinie (S. 3) meint.

[208] Vgl. in diesem Sinne Urteil Prokuratuur (Rn. 49 und die dort angeführte Rechtsprechung).

Kontrollstelle diese Befugnisse bei der Umsetzung der Richtlinie in innerstaatliches Recht vollumfänglich zuerkennen, indem sie sie mit den materiellen und personellen Mitteln ausstatten, die für die Erfüllung ihres Auftrags erforderlich sind.

208. Nach alledem überschreitet die PNR-Richtlinie meiner Ansicht nach nicht die Grenzen des absolut Notwendigen, soweit sie die Übermittlung und automatisierte Verarbeitung der Daten jeder Person gestattet, die dem Begriff „Fluggast" im Sinne von Art. 3 Nr. 4 dieser Richtlinie entspricht.

iv) Zu der Frage, ob die Vorabüberprüfung von Fluggästen hinreichend klar und präzise und auf das absolut Notwendige beschränkt ist (sechste Vorlagefrage)

209. Mit seiner sechsten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof wissen, ob die in Art. 6 der PNR-Richtlinie genannte Vorabüberprüfung mit den Art. 7, 8 und 52 Abs. 1 der Charta vereinbar ist. Obwohl der Wortlaut dieser Frage auf den mit der Vorabüberprüfung verbundenen systematischen und allgemeinen Charakter der automatisierten Verarbeitung der PNR-Daten aller Fluggäste abstellt, geht aus den Gründen der Vorlageentscheidung hervor, dass der Verfassungsgerichtshof den Gerichtshof um eine umfassendere Beurteilung der Frage ersucht, ob die Erfordernisse der Gesetzmäßigkeit und der Verhältnismäßigkeit im Kontext einer solchen Verarbeitung eingehalten werden. Ich werde diese Beurteilung im Folgenden vornehmen, gleichzeitig aber auf die Analyse verweisen, die anlässlich der Prüfung der vierten Vorlagefrage hinsichtlich der fehlenden Zielgerichtetheit der automatisierten Verarbeitung durchgeführt worden ist.

210. Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie sieht vor, dass die PNR-Zentralstellen vor der planmäßigen Ankunft von Fluggästen in einem Mitgliedstaat oder vor ihrem Abflug von einem Mitgliedstaat eine Vorabüberprüfung dieser Fluggäste vornehmen. Mit der Überprüfung sollen diejenigen Personen ermittelt werden, die von den zuständigen Behörden genauer überprüft werden müssen, „da sie möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind". Nach Art. 6 Abs. 6 der PNR-Richtlinie übermittelt die PNR-Zentralstelle eines Mitgliedstaats die PNR-Daten der im Rahmen dieser Überprüfung ermittelten Personen oder die Ergebnisse der Verarbeitung dieser Daten „zur weiteren Überprüfung" an die zuständigen Behörden gemäß Art. 7 desselben Mitgliedstaats.

211. Gemäß Art. 6 Abs. 3 der PNR-Richtlinie werden die Vorabüberprüfungen nach Abs. 2 Buchst. a dieses Artikels durchgeführt, indem die PNR-Daten mit „maßgeblichen" Datenbanken (Art. 6 Abs. 3 Buchst. a) oder anhand im Voraus festgelegter Kriterien (Art. 6 Abs. 3 Buchst. b) abgeglichen werden.

212. Bevor ich mit der Prüfung dieser beiden Arten von Datenverarbeitungen beginne, stelle ich fest, dass sich aus dem Wortlaut des vorerwähnten Art. 6 Abs. 3 nicht eindeutig ergibt, ob die Mitgliedstaaten vorsehen müssen, dass die Vorabüberprüfung von Fluggästen erfolgt, indem systematisch und in allen Fällen sowohl die eine als auch die andere automatisierte Analyse durchgeführt wird, oder ob sie, wie die Verwendung des Verbs „dürfen" und der disjunktiven Konjunktion „oder" zu untermauern scheint, ermächtigt sind, ihre Systeme so auszugestalten, dass beispielsweise die in Art. 6 Abs. 3 Buchst. b vorgesehene Prüfung bestimmten Fällen vorbehalten wird. Nach dem Vorschlag für eine PNR-Richtlinie wurde diese Prüfung lediglich im Rahmen der Bekämpfung schwerer grenzüberschreitender Kriminalität vorgenommen [209].

[209] Vgl. Art. 4 Abs. 2 Buchst. a des Vorschlags für eine PNR-Richtlinie.

213. Wie die Kommission bin ich der Ansicht, dass die Mitgliedstaaten, wie u. a. aus der Systematik der PNR-Richtlinie hervorgeht, aus Gründen, die auch mit dem Erfordernis zusammenhängen, eine möglichst einheitliche Anwendung des Systems zur Verarbeitung von PNR-Daten der Union sicherzustellen, verpflichtet sind, beide Arten automatisierter Verarbeitungen vorzusehen. Dies bedeutet jedoch nicht, dass die Mitgliedstaaten nicht befugt – und, um zu gewährleisten, dass die mit der gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie vorgenommenen Vorabüberprüfung verbundene Datenverarbeitung auf das absolut Notwendige beschränkt ist, sogar verpflichtet – sind, die Analyse gemäß Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie nach Maßgabe ihrer Ergebnisse in Sachen Wirksamkeit für die einzelnen in dieser Richtlinie genannten strafbaren Handlungen zu begrenzen und sie gegebenenfalls lediglich bestimmten strafbaren Handlungen vorzubehalten. Dafür spricht der siebte Erwägungsgrund der PNR-Richtlinie, in dem es heißt: „Damit die Verarbeitung von PNR-Daten … auf das Erforderliche beschränkt bleibt, sollten die Aufstellung und Anwendung von Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, beschränkt werden."

– *Zum Abgleich mit Datenbanken im Sinne von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie*

214. Im ersten Teil der Vorabüberprüfung, die die PNR-Zentralstellen gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie vornehmen, werden die PNR-Daten nach Abs. 3 Buchst. a dieses Artikels mit Datenbanken abgeglichen („data matching"), um etwaige Treffer („hits") zu ermitteln. Diese Hits müssen nach Art. 6 Abs. 5 der PNR-Richtlinie von den PNR-Zentralstellen überprüft und gegebenenfalls als „Match" gekennzeichnet werden, bevor sie an die zuständigen Behörden übermittelt werden.

215. Wie der Gerichtshof in Rn. 172 des Gutachtens 1/15 anerkannt hat, hängt der Umfang des Eingriffs derartiger automatisierter Analysen in die in den Art. 7 und 8 der Charta niedergelegten Rechte im Wesentlichen von den Datenbanken ab, auf denen diese Analysen beruhen. Es ist daher von größter Bedeutung, dass die Bestimmungen, die solche Datenverarbeitungen vorsehen, hinreichend klar und präzise angeben, mit welchen Datenbanken die zu verarbeitenden Daten abgeglichen werden dürfen.

216. Gemäß Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie gleichen die PNR-Zentralstellen die PNR-Daten mit „maßgeblichen Datenbanken"[210] im Hinblick auf die mit dieser Richtlinie verfolgten Ziele ab. In der besagten Vorschrift wird auch eine spezifische Kategorie von Datenbanken erwähnt, nämlich solche betreffend „Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind", die der Unionsgesetzgeber somit ausdrücklich als „maßgeblich" im Sinne der Vorschrift einstufen wollte.

217. Abgesehen von dieser Klarstellung wird der Begriff „maßgebliche Datenbanken" nicht weiter erläutert. Es wird insbesondere nicht angegeben, ob die für den Abgleich der PNR-Daten verwendeten Datenbanken, um als „maßgeblich" angesehen werden zu können, von Strafverfolgungsbehörden oder ganz allgemein von Behörden verwaltet werden müssen oder ob sie ihnen nur direkt oder indirekt zugänglich sein müssen. Auch die Art der Daten, die solche Datenbanken enthalten können, und ihr Verhältnis zu den mit der PNR-Richtlinie verfolgten

[210] Während es in der französischen Sprachfassung von Art. 6 Abs. 3 Buchst. a „base de données utiles" (nützliche Datenbanken) heißt, stellt diese Vorschrift in den meisten anderen Sprachfassungen eher auf „einschlägige Datenbanken" ab: vgl. u. a. die spanische („pertinentes"), die deutsche („maßgeblich"), die englische („relevant"), die italienische („pertinenti"), die niederländische („relevant") und die portugiesische („relevantes") Sprachfassung.

Zielen werden nicht präzisiert[211]. Darüber hinaus geht aus dem Wortlaut von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie hervor, dass sowohl nationale und Datenbanken der Union als auch internationale Datenbanken als „maßgebliche Datenbanken" eingestuft werden können, was die Liste der potenziellen Zieldatenbanken zusätzlich erweitert und die Offenheit dieses Begriffs erhöht[212].

218. Daher hat der Gerichtshof Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie und insbesondere den Begriff „maßgebliche Datenbanken" in Anwendung des in Nr. 151 der vorliegenden Schlussanträge in Erinnerung gerufenen allgemeinen Auslegungsgrundsatzes soweit wie möglich im Einklang mit den sich aus der Charta ergebenden Erfordernissen der Klarheit und Präzision auszulegen. Da diese Vorschrift einen Eingriff in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte vorsieht, muss sie außerdem eng und unter Berücksichtigung des Erfordernisses, ein hohes Schutzniveau für diese Grundrechte zu gewährleisten, das u. a. im 15. Erwägungsgrund der PNR-Richtlinie aufgestellt wird, ausgelegt werden. Ferner ist sie im Licht des in Art. 1 Abs. 2 der PNR-Richtlinie aufgestellten Grundsatzes der Zweckbindung bei der Verarbeitung von PNR-Daten auszulegen.

219. Unter Berücksichtigung der vorstehenden Kriterien ist der Begriff „maßgebliche Datenbanken" meiner Ansicht nach dahin auszulegen, dass er sich nur auf nationale Datenbanken, die von den zuständigen Behörden gemäß Art. 7 Abs. 1 der PNR-Richtlinie verwaltet werden, sowie auf Datenbanken der Union und internationale Datenbanken bezieht, die von diesen Behörden im Rahmen ihres Auftrags direkt betrieben werden. Die Datenbanken müssen außerdem in einem unmittelbaren und engen Zusammenhang mit den von der PNR-Richtlinie verfolgten Zwecken der Bekämpfung von Terrorismus und schwerer Kriminalität stehen, was voraussetzt, dass sie zu diesen Zwecken entwickelt worden sind. So ausgelegt, bezieht sich der Begriff hauptsächlich, wenn nicht ausschließlich auf die in Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie ausdrücklich erwähnten Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind.

220. Vom Begriff „maßgebliche Datenbanken" sind generell Datenbanken ausgeschlossen, die von den Nachrichtendiensten der Mitgliedstaaten verwaltet oder betrieben werden, es sei denn, sie erfüllen in jeder Hinsicht die Voraussetzung eines engen Zusammenhangs mit den von der PNR-Richtlinie verfolgten Zielen und der fragliche Mitgliedstaat erkennt seinen Nachrichtendiensten spezifische Befugnisse im Strafverfolgungsbereich zu[213].

221. Die oben vorgeschlagene Auslegung steht im Einklang mit den vom Gerichtshof in Rn. 172 des Gutachtens 1/15 formulierten Empfehlungen.

211 So wie er abgefasst ist, scheint Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie Analysen in Form einer Datengewinnung durch Abgleich mit sehr unterschiedlichen Daten zu gestatten, sofern die Gewinnung auf die Verfolgung der Ziele dieser Richtlinie ausgerichtet ist. Zu den Risiken im Zusammenhang mit „data mining" im Bereich der PNR-Daten vgl. Korff-Bericht, S. 77. Der EDSB hat in seiner Stellungnahme vom 25. März 2011 (Nr. 18) nachdrücklich darauf hingewiesen, dass die Angabe, mit welchen Datenbanken die PNR-Daten abgeglichen werden dürfen, ungenau und wenig vorhersehbar sei.

212 Der vage und offene Charakter des Wortlauts von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie äußert sich in einer sehr unterschiedlichen Umsetzung in nationales Recht, die von einer engen Auslegung des Begriffs „maßgebliche Datenbanken", bei der die vorgesehene Analyse auf einen Abgleich mit den in dieser Vorschrift ausdrücklich erwähnten Datenbanken beschränkt ist (das ist der Fall bei der Bundesrepublik Deutschland, wie aus den von ihrer Regierung vor dem Gerichtshof abgegebenen Erklärungen hervorgeht), bis zu einer weiteren Auslegung reicht, die alle Datenbanken umfasst, die den zuständigen Behörden im Rahmen ihres Auftrags zur Verfügung stehen oder zugänglich sind (in diesem Sinne ist u. a. Art. 24 § 1 Nr. 1 des PNR-Gesetzes abgefasst).

213 Nach meinem Dafürhalten darf sich ein Mitgliedstaat auf der Grundlage von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie keinesfalls für verpflichtet halten, seiner PNR-Zentralstelle zu gestatten, die PNR-Daten systematisch mit von seinen Nachrichtendiensten verwalteten „maßgeblichen Datenbanken" im Sinne dieser Vorschrift abzugleichen.

222. Auch so ausgelegt lässt sich mit Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie jedoch nicht hinreichend präzise feststellen, welche Datenbanken von den Mitgliedstaaten im Rahmen des Abgleichs mit den PNR-Daten verwendet werden, so dass nicht davon ausgegangen werden kann, dass er die sich aus Art. 52 Abs. 1 der Charta in der Auslegung durch den Gerichtshof ergebenden Anforderungen erfüllt. Die Vorschrift ist daher dahin auszulegen, dass sie die Mitgliedstaaten dazu verpflichtet, im Rahmen der Umsetzung der PNR-Richtlinie in nationales Recht eine Liste mit den entsprechenden Datenbanken zu veröffentlichen und auf dem neuesten Stand zu halten. Es wäre darüber hinaus wünschenswert, dass auf Unionsebene eine Liste mit „maßgeblichen" Datenbanken im Sinne von Art. 6 Abs. 3 Buchst. a der PNR-Richtlinie, die von der Union in Zusammenarbeit mit den Mitgliedstaaten verwaltet werden, und internationalen Datenbanken erstellt wird, um die diesbezügliche Praxis der Mitgliedstaaten zu vereinheitlichen.

– *Zum Abgleich der PNR-Daten anhand im Voraus festgelegter Kriterien*

223. Der zweite Teil der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie besteht in einer automatisierten Analyse anhand im Voraus festgelegter Kriterien. Im Rahmen dieser Analyse werden die PNR-Daten – hauptsächlich zu prädiktiven Zwecken – durch die Anwendung von Algorithmen verarbeitet, die es ermöglichen sollen, Fluggäste zu „ermitteln", die an terroristischen Straftaten oder an schwerer Kriminalität beteiligt sein könnten. Dabei nimmt die PNR-Zentralstelle im Wesentlichen ein Profiling vor[214]. Da eine solche Verarbeitung für die durch den Algorithmus ermittelten Personen weitreichende Konsequenzen haben kann[215], erfordert sie präzise Rahmenbestimmungen sowohl für die Modalitäten ihrer Durchführung als auch für die Garantien, die mit ihr einhergehen müssen. Wie der Gerichtshof in Rn. 172 des Gutachtens 1/15 bemerkt hat, hängt der Umfang des Eingriffs derartiger Analysen in die in den Art. 7 und 8 der Charta niedergelegten Rechte nämlich im Wesentlichen von den angewandten im Voraus festgelegten Modellen und Kriterien ab.

224. Ich stelle insoweit erstens fest, dass die im Voraus festgelegten Kriterien, anhand deren die in Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie vorgesehene Vorabüberprüfung durchgeführt wird, gemäß Art. 6 Abs. 4 Satz 2 dieser Richtlinie „zielgerichtet, verhältnismäßig und bestimmt" sein müssen. Das erste Erfordernis bezieht sich auf das Ziel der in Abs. 2 Buchst. a des Artikels vorgesehenen Vorabüberprüfung, nämlich die Ermittlung derjenigen Personen, die von den zuständigen Behörden genauer überprüft werden müssen, und trägt daher der vom Gerichtshof im Gutachten 1/15 hervorgehobenen Notwendigkeit Rechnung, dass es mit den verwendeten Kriterien gelingt, Personen zu „identifizieren", gegen die ein „begründeter Verdacht" der Beteiligung an terroristischen Straftaten oder schwerer Kriminalität bestehen könnte[216]. Eine solche „Identifizierung" setzt die Anwendung abstrakter Prüfkriterien oder – um einen Ausdruck

214 Art. 3 Nr. 4 der Polizei-Richtlinie definiert „Profiling" als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen". Die gleiche Definition ist in Art. 4 Nr. 4 der DSGVO und Nr. 1 Buchst. c des Anhangs zur Empfehlung CM/Rec(2021)8 des Ministerkomitees des Europarates vom 3. November 2021 über den Schutz von Personen bei der automatisierten Verarbeitung personenbezogener Daten im Rahmen der Profilerstellung, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148, (im Folgenden: Empfehlung von 2021 über die Profilerstellung) enthalten.

215 Nr. 1 Buchst. j Ziff. i der Empfehlung von 2021 über die Profilerstellung definiert als „hochriskante Verarbeitung zur Profilerstellung" eine „Profilerstellung, deren Funktionsweise Rechtswirkungen auslöst oder die erhebliche Auswirkungen auf die betroffene Person oder die durch die Verarbeitung zur Profilerstellung ermittelte Personengruppe hat".

216 Vgl. Gutachten 1/15 (Rn. 172).

in der Empfehlung von 2021 über die Profilerstellung zu verwenden – von „Profilen“ [217] voraus, mittels derer sich die PNR-Daten „filtern“ lassen, um diejenigen Fluggäste zu ermitteln, die diese Kriterien erfüllen und daher möglicherweise genauer überprüft werden müssen. Die PNR-Richtlinie gestattet hingegen kein individuelles Profiling aller Fluggäste, deren Daten analysiert werden, beispielsweise indem jedem von ihnen eine Risikokategorie auf einer im Voraus festgelegten Skala zugewiesen wird, da dies andernfalls sowohl gegen Art. 6 Abs. 4 der Richtlinie verstieße als auch die Grenzen verletzen würde, die der Gerichtshof der automatisierten Verarbeitung von PNR-Daten im Gutachten 1/15 gesetzt hat.

225. Nach Art. 6 Abs. 4 Satz 2 müssen die in Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie genannten im Voraus festgelegten Kriterien außerdem „bestimmt“ [218], nämlich an den verfolgten Zweck angepasst und für diesen relevant, sowie „verhältnismäßig“ [219] sein, d. h. sie dürfen seine Grenzen nicht überschreiten. Um diesen Anforderungen zu genügen, insbesondere „[d]amit die Verarbeitung von PNR-Daten … auf das Erforderliche beschränkt bleibt“, sieht der siebte Erwägungsgrund der PNR-Richtlinie, wie ich bereits hervorgehoben habe, vor, dass „die Aufstellung und Anwendung von Prüfkriterien auf terroristische Straftaten und schwere Kriminalität, für die die Anwendung solcher Kriterien maßgeblich ist, beschränkt werden [sollten]“.

226. Schließlich geht sowohl aus der Präambel und den Bestimmungen der PNR-Richtlinie als auch aus den vom Gerichtshof im Gutachten 1/15 aufgestellten Erfordernissen hervor, dass die in Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie genannten im Voraus festgelegten Kriterien ferner „zuverlässig“ [220] sein müssen, was zum einen bedeutet, dass sie konzipiert werden müssen, um das Fehlerrisiko zu minimieren [221], und zum anderen, dass sie „aktuell“ [222] sein müssen. Art. 6 Abs. 4 Satz 3 der PNR-Richtlinie verpflichtet die Mitgliedstaaten insoweit dazu, sicherzustellen, dass diese Kriterien „von der PNR-Zentralstelle aufgestellt und von ihr in Zusammenarbeit mit den in Artikel 7 genannten zuständigen Behörden regelmäßig überprüft werden“ [223]. Um die Zuverlässigkeit der Kriterien zu gewährleisten und falschpositive Ergebnisse weitestgehend zu begrenzen, ist es, wie die Kommission in Beantwortung einer schriftlichen Frage des Gerichtshofs anerkannt hat, außerdem erforderlich, dass die Kriterien in einer Weise konzipiert werden, die sowohl belastende als auch entlastende Elemente berücksichtigt.

227. Zweitens verbietet die PNR-Richtlinie ausdrücklich diskriminierendes Profiling. So sieht Art. 6 Abs. 4 Satz 1 dieser Richtlinie vor, dass die Vorabüberprüfung anhand im Voraus festgelegter Kriterien gemäß Abs. 3 Buchst. b „in nichtdiskriminierender Weise“ erfolgt. Insoweit ist klarzustellen, dass, auch wenn es in Art. 6 Abs. 4 Satz 3 heißt, dass „[d]ie rassische oder ethnische Herkunft, die politischen Meinungen, die religiösen oder weltanschaulichen Überzeugungen, die Mitgliedschaft in einer Gewerkschaft, der Gesundheitszustand, das

[217] Gemäß Nr. 1.1 Buchst. d des Anhangs zur Empfehlung von 2021 über die Profilerstellung bezeichnet der Ausdruck „Profil“ „den einer Person zugewiesenen Datensatz, der eine Personengruppe kennzeichnet oder dazu bestimmt ist, auf eine Person angewandt zu werden“. Wie es im Bericht über die Entwicklung der Lage nach der Annahme der Empfehlung (2010)13 über die Profilerstellung (https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b, S. 21), die der Annahme der Empfehlung von 2021 über die Profilerstellung vorausgegangen ist, heißt, ist der Begriff „Profil“ in Systemen, in denen – wie in der PNR-Richtlinie – zwischen Vorgängen zur Erstellung von Profilen (vgl. u. a. Art. 6 Abs. 2 Buchst. b dieser Richtlinie) und solchen unterschieden wird, die ihn anwenden, nach wie vor sinnvoll und ermöglicht „eine Transparenz der Kriterien, die in einem zweiten Schritt durch das Profiling angewandt werden“.

[218] Vgl. Art. 6 Abs. 4 der PNR-Richtlinie und Gutachten 1/15 (Rn. 172).

[219] Vgl. Art. 6 Abs. 4 der PNR-Richtlinie.

[220] Vgl. Gutachten 1/15 (Rn. 172).

[221] Vgl. siebter Erwägungsgrund der PNR-Richtlinie.

[222] Vgl. Gutachten 1/15 (Rn. 174).

[223] Die gleiche Anforderung ist in Rn. 174 des Gutachtens 1/15 enthalten.

Sexualleben oder die sexuelle Orientierung einer Person … unter keinen Umständen als Grundlage“ für diese Kriterien dienen dürfen, das allgemeine Verbot diskriminierender Profilerstellung so zu verstehen ist, dass es alle in Art. 21 der Charta erwähnten Diskriminierungsgründe und sogar solche umfasst, die nicht ausdrücklich erwähnt werden [224].

228. Drittens geht sowohl aus dem Wortlaut von Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie als auch aus dem in dieser Richtlinie vorgesehenen System von Garantien, die mit der automatisierten Verarbeitung von PNR-Daten einhergehen, hervor, dass die Funktionsweise der Algorithmen, die im Rahmen der in Art. 6 Abs. 3 Buchst. b vorgesehenen Analyse verwendet werden, transparent und das Ergebnis ihrer Anwendung nachvollziehbar sein muss. Dieses Transparenzerfordernis bedeutet natürlich nicht, dass die verwendeten „Profile“ veröffentlicht werden müssen. Es verlangt jedoch, dass die Erkennbarkeit der algorithmischen Entscheidungsfindung gewährleistet ist. Zum einen schließt das Erfordernis, wonach die Kriterien, anhand deren die Analyse zu erfolgen hat, „im Voraus festgelegt“ werden müssen, nämlich aus, dass sich die Kriterien ohne menschlichen Eingriff ändern lassen, und steht daher der Nutzung von KI-Technologien, die auch als „machine learning“ [225] bezeichnet werden und einen höheren Detaillierungsgrad aufweisen können, aber selbst für Betreiber, die eine automatisierte Verarbeitung vorgenommen haben, schwer zu interpretieren sind [226], entgegen. Zum anderen muss – was die in Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie genannte Analyse angeht – gemäß der in Art. 6 Abs. 5 und 6 dieser Richtlinie beschriebenen Garantie, wonach jeder einzelne Treffer bei der automatisierten Verarbeitung von PNR-Daten nach Maßgabe von Art. 6 Abs. 2 Buchst. a auf andere, nicht automatisierte Art individuell überprüft wird, nachvollzogen werden können, weshalb das Programm zu einem solchen Treffer gelangt ist, was sich u. a. dann nicht gewährleisten lässt, wenn Selbstlernsysteme verwendet werden. Gleiches gilt für die Kontrolle der Rechtmäßigkeit dieser Analyse, auch in Bezug auf den nicht diskriminierenden Charakter der erzielten Ergebnisse, mit der der Datenschutzbeauftragte und die nationale Kontrollstelle gemäß Art. 6 Abs. 7 bzw. Art. 15 Abs. 3 Buchst. b der PNR-Richtlinie betraut sind. Die Transparenz der Funktionsweise der verwendeten Algorithmen ist auch eine notwendige Bedingung, um den Betroffenen die Ausübung ihrer Beschwerderechte und ihres Rechts auf effektiven gerichtlichen Rechtsschutz zu ermöglichen.

– *Zu den Garantien, die mit der automatisierten Verarbeitung von PNR-Daten einhergehen*

229. Ich habe bereits einige der Garantien erwähnt, die mit der automatisierten Verarbeitung von PNR-Daten im Rahmen der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie einhergehen und die vom Gerichtshof im Gutachten 1/15 aufgestellten Anforderungen erfüllen, nämlich das Verbot der Verarbeitung auf der Grundlage im Voraus festgelegter diskriminierender Kriterien (Art. 6 Abs. 4 Satz 1 und 4 der PNR-Richtlinie; Gutachten 1/15, Rn. 172), die regelmäßige Aktualisierung der im Voraus festgelegten Kriterien, anhand deren die in Art. 6 Abs. 3 Buchst. b dieser Richtlinie genannte Vorabüberprüfung vorgenommen werden muss (Art. 6 Abs. 4 Satz 3 der PNR-Richtlinie; Gutachten 1/15, Rn. 174), die Überprüfung jedes

224 Sämtliche in Art. 21 der Charta enthaltenen Diskriminierungsgründe werden im 20. Erwägungsgrund der PNR-Richtlinie wiedergegeben. Eine Angleichung an die in Art. 21 genannte Liste der verbotenen Diskriminierungsgründe war von der FRA in ihrem Gutachten 1/2011 (S. 8) vorgeschlagen worden.

225 Gemäß Nr. 1.1 Buchst. g des Anhangs zur Empfehlung von 2021 über die Profilerstellung bezeichnet der Ausdruck „machine learning“ „eine Verarbeitung unter Verwendung besonderer KI-Methoden auf der Grundlage statistischer Ansätze, um Computern die Fähigkeit zu geben, aus Daten zu ‚lernen‘, d. h. ihre Leistungsfähigkeit bei der Lösung von Aufgaben zu verbessern, ohne für die einzelnen Aufgaben explizit programmiert zu werden“.

226 Zu der Frage, wie sich die Undurchsichtigkeit der algorithmischen Systeme auf die Möglichkeit einer menschlichen Kontrolle zur Vermeidung der schädlichen Auswirkungen dieser Systeme und ihrer negativen Folgen für die Menschenrechte auswirkt, vgl. Empfehlung CM/Rec(2020)1 des Ministerkomitees des Europarates an die Mitgliedstaaten über die Folgen der algorithmischen Systeme für die Menschenrechte.

einzelnen Treffers bei der automatisierten Verarbeitung von PNR-Daten mit nicht automatisierten Mitteln (Art. 6 Abs. 5 und 6 der PNR-Richtlinie; Gutachten 1/15, Rn. 173) und die Kontrolle der Rechtmäßigkeit dieser Verarbeitung durch den Datenschutzbeauftragten und die nationale Kontrollstelle (Art. 6 Abs. 7 und Art. 15 Abs. 3 Buchst. b der PNR-Richtlinie). In diesem Zusammenhang ist es äußerst wichtig, dass sich die Kontrolle durch eine unabhängige Stelle wie die in Art. 15 der PNR-Richtlinie genannte Stelle zum einen auf jeden Aspekt der automatisierten Verarbeitung von PNR-Daten, einschließlich der Ermittlung der für den Abgleich im Sinne von Art. 6 Abs. 3 Buchst. a der Richtlinie verwendeten Datenbanken und der Erarbeitung der bei der Analyse gemäß deren Art. 6 Abs. 3 Buchst. b angewandten im Voraus festgelegten Kriterien, beziehen und zum anderen sowohl *ex ante* als auch *ex post* ausgeübt werden kann.

230. Hervorzuheben ist, dass die oben genannten Garantien analyseübergreifend als auf beide in Art. 6 Abs. 3 der PNR-Richtlinie erwähnten Analysearten anwendbar verstanden werden sollten, auch wenn das aus dem Wortlaut nicht hervorgeht. So gilt, auch wenn in Art. 6 Abs. 4 Satz 1 der PNR-Richtlinie auf das Erfordernis der Wahrung des Grundsatzes der Nichtdiskriminierung nur in Bezug auf die anhand im Voraus festgelegter Kriterien vorgenommene Vorabüberprüfung hingewiesen wird, dieses Erfordernis in jeder Phase des Prozesses der Verarbeitung von PNR-Daten und somit auch dann, wenn die Daten im Rahmen der Vorabüberprüfung im Sinne von Art. 6 Abs. 3 Buchst. a der Richtlinie mit maßgeblichen Datenbanken abgeglichen werden. Gleiches gilt für das Erfordernis, wonach die im Rahmen der Analyse nach Art. 6 Abs. 3 Buchst. b der PNR-Richtlinie verwendeten im Voraus festgelegten Kriterien zuverlässig sein und aktualisiert werden müssen, das so zu verstehen ist, dass es sich auch auf Daten in den Datenbanken bezieht, die für den in Art. 6 Abs. 3 Buchst. a dieser Richtlinie vorgesehenen Abgleich verwendet werden. Ich stelle insoweit ganz allgemein fest, dass alle Garantien, die für die in der Polizei-Richtlinie vorgesehenen automatisierten Verarbeitungen personenbezogener Daten gelten, auch im Rahmen der PNR-Richtlinie anwendbar sind, da davon auszugehen ist, dass automatisierte Analysen, die im Rahmen der letztgenannten Richtlinie durchgeführt werden, in den Anwendungsbereich der Polizei-Richtlinie fallen.

231. Zu den oben in Nr. 229 aufgeführten Garantien gesellt sich die in Art. 7 Abs. 6 der PNR-Richtlinie vorgesehene Garantie, die zum einen das Verbot, Entscheidungsprozesse ausschließlich auf die Ergebnisse der automatisierten Verarbeitung der PNR-Daten zu stützen, und zum anderen das Verbot der Diskriminierung bei der Verarbeitung und Nutzung dieser Daten ergänzt. So sieht diese Vorschrift vor, dass „[d]ie zuständigen Behörden … Entscheidungen, aus denen sich eine nachteilige Rechtsfolge oder ein sonstiger schwerwiegender Nachteil für die betroffene Person ergibt, unter keinen Umständen allein auf der Grundlage der automatisierten Verarbeitung der PNR-Daten [treffen]“ und dass solche Entscheidungen „[e]benso wenig … aufgrund der rassischen oder ethnischen Herkunft, der politischen Meinungen, der religiösen oder weltanschaulichen Überzeugungen, der Mitgliedschaft in einer Gewerkschaft, des Gesundheitszustands, des Sexuallebens oder der sexuellen Orientierung einer Person getroffen [werden]“. Wie ich in Nr. 227 der vorliegenden Schlussanträge in Bezug auf Art. 6 Abs. 4 Satz 4 der PNR-Richtlinie ausgeführt habe, ist dieser Katalog von Diskriminierungsgründen durch Hinzufügung der in Art. 21 der Charta enthaltenen und der nicht ausdrücklich erwähnten Gründe zu ergänzen.

232. In Bezug auf die Sicherheit der PNR-Daten sieht Art. 6 Abs. 8 der PNR-Richtlinie vor, dass die Speicherung, Verarbeitung und Auswertung dieser Daten durch die PNR-Zentralstelle ausschließlich an einem gesicherten Ort bzw. gesicherten Orten im Hoheitsgebiet der Mitgliedstaaten erfolgt.

– *Ergebnis zur sechsten Vorlagefrage*

233. Nach alledem bin ich vorbehaltlich der u. a. in den Nrn. 213, 219, 220, 222, 227, 228, 230 und 231 der vorliegenden Schlussanträge vorgeschlagenen Auslegungen der Ansicht, dass die automatisierte Verarbeitung von PNR-Daten im Rahmen der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie den Erfordernissen der Klarheit und Präzision genügt und auf das absolut Notwendige beschränkt ist.

v) Zur Aufbewahrung von PNR-Daten (achte Vorlagefrage)

234. Mit seiner achten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof wissen, ob Art. 12 der PNR-Richtlinie in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der Charta dahin auszulegen ist, dass er einzelstaatlichen Rechtsvorschriften entgegensteht, die eine allgemeine Aufbewahrungsdauer für PNR-Daten von fünf Jahren vorsehen, ohne eine Unterscheidung danach vorzunehmen, ob sich im Rahmen der Vorabüberprüfung herausstellt, dass die betroffenen Fluggäste ein Risiko für die öffentliche Sicherheit darstellen können oder nicht.

235. Art. 12 Abs. 1 der PNR-Richtlinie sieht vor, dass die PNR-Daten „für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen beziehungsweise von dem er abgegangen ist“, in einer Datenbank vorgehalten werden. Nach Art. 12 Abs. 2 werden die PNR-Daten nach Ablauf einer „anfänglichen Speicherfrist“ [227] von sechs Monaten durch Unkenntlichmachung bestimmter Daten, mit denen die Identität der betreffenden Person unmittelbar festgestellt werden könnte, depersonalisiert. Gemäß Art. 12 Abs. 3 ist die Offenlegung der vollständigen PNR-Daten, einschließlich der unkenntlich gemachten Elemente, nach Ablauf der Frist von sechs Monaten nur zulässig, wenn „berechtigter Grund“ zu der Annahme besteht, dass dies für die Zwecke des Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie erforderlich ist und dies genehmigt wird durch eine Justizbehörde oder eine andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind. Schließlich sieht Art. 12 Abs. 4 vor, dass die PNR-Daten nach Ablauf der fünfjährigen Frist nach Abs. 1 dauerhaft gelöscht werden.

236. Aus dem Vorstehenden geht hervor, dass die PNR-Richtlinie die Aufbewahrung von PNR-Daten, einschließlich der Dauer dieser Aufbewahrung, selbst regelt und auf fünf Jahre festsetzt [228], so dass die Mitgliedstaaten insoweit grundsätzlich keinerlei Ermessensspielraum haben, was von der Kommission im Übrigen bestätigt worden ist. Daher wird der Gerichtshof, worauf ich bereits hingewiesen habe, mit der achten Vorlagefrage, auch wenn sie wie eine Auslegungsfrage formuliert ist, in Wirklichkeit aufgefordert, sich zur Vereinbarkeit dieser Regelung mit der Charta zu äußern.

237. Es ist ein allgemeiner Grundsatz auf dem Gebiet des Schutzes personenbezogener Daten, dass diese Daten nicht in einer Form gespeichert werden dürfen, die die direkte oder indirekte Identifizierung der betroffenen Personen über einen längeren Zeitraum ermöglicht, als er für die

[227] Diese Definition ist im 25. Erwägungsgrund der PNR-Richtlinie enthalten.

[228] Mit dem Wortlaut des 37. Erwägungsgrundes der PNR-Richtlinie, wonach diese „die Speicherfrist für die PNR-Daten bei den PNR-Zentralstellen auf *maximal fünf Jahre* [beschränkt], nach deren Ablauf die Daten gelöscht werden sollten“ (Hervorhebung nur hier), lässt sich der klare Wortlaut von Art. 12 Abs. 1 der Richtlinie nach meinem Dafürhalten nicht in Frage stellen.

Zwecke, für die sie verarbeitet werden, erforderlich ist [229]. Darüber hinaus muss eine Regelung, die eine Vorratsspeicherung personenbezogener Daten vorsieht, nach ständiger Rechtsprechung stets objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen [230].

238. Im Gutachten 1/15 hat der Gerichtshof in Bezug auf die bei der Einreise nach Kanada erhobenen Daten die Auffassung vertreten, dass der erforderliche Zusammenhang zwischen den PNR-Daten und dem mit dem Entwurf eines PNR-Abkommens Kanada–EU verfolgten Ziel für alle Fluggäste feststand, solange sie sich im Hoheitsgebiet dieses Drittlands befanden [231]. Bei Fluggästen, die aus Kanada ausgereist sind und bei denen eine Gefahr im Bereich des Terrorismus oder grenzübergreifender schwerer Kriminalität weder bei ihrer Ankunft in noch bis zu ihrer Ausreise aus diesem Drittland festgestellt worden war, bestand ein solcher Zusammenhang, der die Speicherung ihrer PNR-Daten rechtfertigen würde, sei er auch mittelbarer Art, nach Ansicht des Gerichtshofs hingegen nicht [232]. Der Gerichtshof hat gleichwohl festgestellt, dass eine solche Speicherung allerdings zulässig sein kann, wenn es „in konkreten Fällen … objektive Anhaltspunkte dafür [gibt], dass von bestimmten Fluggästen auch nach ihrer Ausreise aus Kanada eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte“ [233].

239. Übertragen auf den Kontext der PNR-Richtlinie, würden die vom Gerichtshof im Gutachten 1/15 aufgestellten Grundsätze bedeuten, dass die bei der Einreise in die Union erhobenen PNR-Daten zu Drittstaatsflügen und die bei der Einreise in den betreffenden Mitgliedstaat erhobenen PNR-Daten zu EU-Flügen nach ihrer Vorabanalyse im Sinne von Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie nur gespeichert werden dürfen, solange sich die betreffenden Fluggäste im Unionsgebiet oder im Hoheitsgebiet dieses Mitgliedstaats aufhalten. Die bei der Ausreise aus der Union erhobenen PNR-Daten zu Drittstaatsflügen und die bei der Ausreise aus dem betreffenden Mitgliedstaat erhobenen PNR-Daten zu EU-Flügen dürften nach der Vorabanalyse grundsätzlich nur im Fall von Fluggästen gespeichert werden, bei denen es objektive Anhaltspunkte dafür gibt, dass von ihnen eine Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und schwerer Kriminalität ausgehen könnte [234].

240. Die Regierungen und Organe, die Erklärungen vor dem Gerichtshof abgegeben haben, treten einer Übertragung der im Gutachten 1/15 auf dem Gebiet der Speicherung von PNR-Daten aufgestellten Grundsätze auf die vorliegende Rechtssache grundsätzlich entgegen. Insoweit ist zwar nicht ausgeschlossen, dass die Tatsache, dass der Gerichtshof auf ein Kriterium im Zusammenhang mit dem Aufenthalt der betreffenden Person im kanadischen Hoheitsgebiet zurückgegriffen hat, möglicherweise durch den Umstand beeinflusst worden ist, dass er es mit einer Speicherung personenbezogener Daten im Hoheitsgebiet eines Drittlands zu tun hatte. Es ist auch möglich, dass die Anwendung eines solchen Kriteriums im Kontext der PNR-Richtlinie konkret in einem Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten zum Ausdruck kommen kann, der für bestimmte Personengruppen, insbesondere solche, die ihren ständigen Wohnsitz in der Union haben und sich innerhalb dieser

229 Vgl. – zur Verarbeitung personenbezogener Daten zwecks Ermittlung, Verhütung, Verfolgung oder Aufdeckung von Straftaten – Art. 4 Abs. 1 Buchst. e und 26. Erwägungsgrund der Polizei-Richtlinie. Vgl. – allgemeiner – Art. 5 Abs. 1 Buchst. e der DSGVO und Art. 5 Abs. 4 Buchst. e des modernisierten Übereinkommens Nr. 108.

230 Vgl. Urteile Schrems I (Rn. 93) und Tele2 Sverige (Rn. 110), Gutachten 1/15 (Rn. 191) sowie Urteil La Quadrature du Net (Rn. 133).

231 Vgl. Gutachten 1/15 (Rn. 197).

232 Vgl. Gutachten 1/15 (Rn. 205).

233 Vgl. Gutachten 1/15 (Rn. 207).

234 Hierbei würde es sich um eine analoge Anwendung der Rn. 187 ff. des Gutachtens 1/15 handeln, da sich dieses nur auf den Fall von PNR-Daten bezog, die bei der Einreise in das kanadische Hoheitsgebiet erhoben wurden.

fortbewegen oder nach einem Aufenthalt im Ausland zurückkehren, potenziell einschneidender ist. Und schließlich trifft es zu, dass dieses Kriterium, zumindest für EU-Flüge, schwierig in die Praxis umzusetzen sein könnte, wie einige Mitgliedstaaten und der Rat hervorgehoben haben.

241. Auch wenn der Wunsch besteht, das Kriterium, auf das der Gerichtshof im Gutachten 1/15 zurückgegriffen hat, auszuschließen, verstößt eine Speicherung sämtlicher PNR-Daten aller Fluggäste – unabhängig vom Ergebnis der in Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie genannten Vorabüberprüfung und ohne dass nach Maßgabe der Gefahr im Bereich des Terrorismus oder schwerer Kriminalität auf der Grundlage objektiver und überprüfbarer Kriterien unterschieden wird – gleichwohl gegen die in Nr. 237 der vorliegenden Schlussanträge in Erinnerung gerufene ständige Rechtsprechung des Gerichtshofs, die dieser in seinem Gutachten zur Anwendung gelangen lassen wollte. Mit den in den Nrn. 201 bis 203 der vorliegenden Schlussanträge im Rahmen der Prüfung der vierten Vorlagefrage dargelegten Erwägungen lassen sich aus meiner Sicht zwar die allgemeine und unterschiedslose Übermittlung von PNR-Daten sowie deren automatisierte Verarbeitung im Rahmen der in Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie vorgesehenen Vorabüberprüfung rechtfertigen, sie allein können nach meinem Dafürhalten – selbst nach einer solchen Überprüfung – aber keine allgemeine und unterschiedslose Speicherung dieser Daten rechtfertigen.

242. Ich stelle darüber hinaus fest, dass die gleiche Aufbewahrungsfrist von fünf Jahren sowohl für die Bekämpfung des Terrorismus oder für die Bekämpfung schwerer Kriminalität als auch – im Rahmen des letztgenannten Zwecks – ausnahmslos für alle in Anhang II aufgeführten strafbaren Handlungen angewandt wird. Wie aus den in Nr. 121 der vorliegenden Schlussanträge angestellten Überlegungen hervorgeht, ist diese Liste ausgesprochen lang und umfasst Straftaten unterschiedlicher Typologie und Schwere. Insoweit ist festzuhalten, dass die Rechtfertigung im Zusammenhang mit der Dauer und der Komplexität der Ermittlungen, die von fast allen Mitgliedstaaten und Organen vorgebracht worden ist, die im vorliegenden Verfahren Erklärungen abgegeben haben, konkret nur für terroristische Straftaten und einige strafbare Handlungen mit eindeutig grenzüberschreitendem Charakter wie beispielsweise Menschenhandel oder Handel mit Drogen sowie ganz allgemein für bestimmte Formen organisierter Kriminalität angeführt wird. Ich weise ferner darauf hin, dass der Gerichtshof im Gutachten 1/15 eine ähnliche Rechtfertigung nur in Bezug auf die Speicherung der PNR-Daten von Fluggästen akzeptiert hat, bei denen eine objektive Gefahr im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität besteht und eine Datenspeicherung von fünf Jahren als nicht über das absolut Notwendige hinausgehend angesehen worden ist [235]. Es ist jedoch angenommen worden, dass diese Rechtfertigung keine „dauerhafte Speicherung der PNR-Daten sämtlicher Fluggäste … zum Zweck eines eventuellen Zugangs zu diesen Daten unabhängig von jedem Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität“ [236] gestatten kann.

243. Richtig ist zwar, dass die PNR-Richtlinie, wie der Rat, das Parlament und die Kommission sowie alle Regierungen, die Erklärungen zur achten Vorlagefrage abgegeben haben, hervorheben, spezifische Garantien sowohl für die Speicherung von PNR-Daten, die nach einer anfänglichen Frist von sechs Monaten teilweise unkenntlich gemacht werden, als auch für ihre Nutzung während der Aufbewahrungsdauer, die strengen Bedingungen unterliegt, vorsieht. Ich stelle jedoch erstens zum einen fest, dass auch der Entwurf eines PNR-Abkommens Kanada–EU ein

[235] Vgl. Gutachten 1/15 (Rn. 209).

[236] Vgl. Gutachten 1/15 (Rn. 205).

System der Anonymisierung von PNR-Daten durch Unkenntlichmachung vorsah[237], und zum anderen, dass eine solche Anonymisierung, wie u. a. der Beratende Ausschuss des Übereinkommens Nr. 108 unterstreicht[238], die Risiken einer längeren Datenaufbewahrungsfrist, etwa einen missbräuchlichen Zugang, zwar eindämmen kann, die unkenntlich gemachten Daten es aber gleichwohl weiterhin ermöglichen, Personen zu identifizieren, und deshalb nach wie vor personenbezogene Daten darstellen, deren Speicherung auch in zeitlicher Hinsicht begrenzt werden muss, um einer allgemeinen permanenten Überwachung vorzubeugen. Eine Aufbewahrungsdauer von fünf Jahren hat insoweit zur Folge, dass eine erhebliche Zahl von Fluggästen, insbesondere solche, die sich innerhalb der Union fortbewegen, quasi dauerhaft registriert werden können. Zweitens weise ich in Bezug auf die Einschränkungen der Datennutzung darauf hin, dass die Speicherung personenbezogener Daten und der Zugang zu solchen Daten unterschiedliche Eingriffe in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen, die eigenständig gerechtfertigt werden müssen. Auch wenn sich mit strengen Garantien für den Zugang zu den gespeicherten Daten die Auswirkungen einer Überwachungsmaßnahme auf die erwähnten Grundrechte umfassend beurteilen lassen, können die Eingriffe im Zusammenhang mit einer längeren allgemeinen Vorratsspeicherung mit ihnen gleichwohl nicht beseitigt werden.

244. Zum Argument der Kommission, wonach die PNR-Daten aller Fluggäste gespeichert werden müssten, um den PNR-Zentralstellen die Erfüllung des in Art. 6 Abs. 2 Buchst. c der PNR-Richtlinie genannten Auftrags, die Kriterien zu aktualisieren oder neue Kriterien zur Verwendung in gemäß Art. 6 Abs. 3 Buchst. b durchgeführten Überprüfungen aufzustellen, ist zu sagen, dass die Präzisierung dieser Kriterien zwar teilweise von ihrem Abgleich mit „normalen“ Verhaltensweisen abhängt, wie die Kommission geltend macht, ihre Erarbeitung aber gleichwohl auf der Grundlage „krimineller“ Verhaltensweisen zu erfolgen hat. Ein solches Argument, das im Übrigen nur von einer begrenzten Zahl von Mitgliedstaaten vorgebracht wird, kann nach meinem Dafürhalten nicht die entscheidende Bedeutung haben, die ihm die Kommission beizulegen scheint, und für sich allein eine allgemeine Vorratsspeicherung von PNR-Daten sämtlicher Fluggäste in nicht anonymisierter Form rechtfertigen.

245. Unter Berücksichtigung der vorstehenden Erwägungen ist, um eine Auslegung von Art. 12 Abs. 1 der PNR-Richtlinie zu gewährleisten, die mit den Art. 7, 8 und 52 Abs. 1 der Charta im Einklang steht, diese Vorschrift nach meinem Dafürhalten dahin auszulegen, dass das Vorhalten der von den Fluggesellschaften an die PNR-Zentralstelle übermittelten PNR-Daten in einer Datenbank für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen bzw. von dem er abgegangen ist, nach Durchführung der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie nur insoweit zulässig ist, als auf der Grundlage objektiver Kriterien ein Zusammenhang zwischen diesen Daten und der Bekämpfung des Terrorismus oder schwerer Kriminalität festgestellt wird. Eine allgemeine und unterschiedslose Vorratsspeicherung von PNR-Daten in nicht anonymisierter Form lässt sich entsprechend den vom Gerichtshof in seiner Rechtsprechung getroffenen Feststellungen nur bei einer schwerwiegenden Gefahr für die Sicherheit der Mitgliedstaaten rechtfertigen, die sich als tatsächlich und gegenwärtig oder vorhersehbar erweist und beispielsweise mit terroristischen Handlungen zusammenhängt, sofern die Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt wird.

[237] Der Entwurf eines PNR-Abkommens Kanada–EU sah vor, dass Kanada 30 Tage nach Erhalt der PNR-Daten eine Unkenntlichmachung der Namen sämtlicher Fluggäste und zwei Jahre nach diesem Erhalt eine Unkenntlichmachung weiterer ausdrücklich aufgeführter Informationen vornahm; vgl. Art. 16 Abs. 3 des vom Gerichtshof untersuchten Entwurfs eines PNR-Abkommens Kanada–EU und Gutachten 1/15 (Rn. 30).

[238] Vgl. Stellungnahme vom 19. August 2016, S. 9.

246. Die Begrenzung der in Art. 12 Abs. 1 der PNR-Richtlinie vorgesehenen Vorratsdatenspeicherung kann beispielsweise auf einer Risikobewertung oder auf der Erfahrung der zuständigen nationalen Behörden beruhen und sich auf bestimmte Flugverbindungen, festgelegte Reiseschemata, Agenturen, über die Buchungen vorgenommen werden, oder aber auf bestimmte Personenkategorien oder geografische Gebiete beziehen, die auf der Grundlage objektiver und nicht diskriminierender Kriterien ermittelt worden sind, wie der Gerichtshof in seiner Rechtsprechung auf dem Gebiet der Vorratsspeicherung von Metadaten elektronischer Kommunikationen entschieden hat [239]. Darüber hinaus gilt der erforderliche Zusammenhang zwischen den PNR-Daten und dem mit der PNR-Richtlinie verfolgten Ziel entsprechend dem Gutachten 1/15 als nachgewiesen, solange sich die Fluggäste in der Union (oder im betreffenden Mitgliedstaat) befinden bzw. im Begriff sind, diese zu verlassen. Gleiches gilt für die Fluggastdaten, die zu einem überprüften Treffer geführt haben.

247. Zum Abschluss der achten Vorlagefrage möchte ich den Vorschriften über den Zugang zu PNR-Daten und ihre Nutzung nach Durchführung der in Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie genannten Vorabüberprüfung und vor ihrer Anonymisierung nach Ablauf der in Art. 12 Abs. 2 der PNR-Richtlinie vorgesehenen anfänglichen Speicherfrist von sechs Monaten einige Überlegungen widmen.

248. Aus einer Auslegung von Art. 6 Abs. 2 Buchst. b in Verbindung mit Art. 12 Abs. 3 der PNR-Richtlinie geht hervor, dass den zuständigen Behörden während dieser anfänglichen Frist nicht anonymisierte PNR-Daten oder die Ergebnisse ihrer Verarbeitung nach der erstgenannten Vorschrift zur Verfügung gestellt werden können, ohne dass die in den Buchst. a und b der letztgenannten Vorschrift festgelegten Voraussetzungen erfüllt sind [240]. Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie sieht nämlich lediglich vor, dass Anfragen zuständiger Behörden hinsichtlich einer solchen Verarbeitung und Zurverfügungstellung „gebührend begründet“ werden und „auf einer hinreichenden Grundlage“ beruhen müssen.

249. Nach einer ständigen Rechtsprechung, die der Gerichtshof im Gutachten 1/15 in Erinnerung gerufen hat, darf sich eine Unionsregelung nicht darauf beschränken, dass der Zugang zu rechtmäßig gespeicherten personenbezogenen Daten durch eine Behörde einem der in der Regelung genannten Zweck zu entsprechen hat, sondern muss auch die materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung der Daten festlegen [241], um diese insbesondere vor Missbrauchsrisiken zu schützen [242]. In besagtem Gutachten hat der Gerichtshof entschieden, dass die Verwendung der PNR-Daten nach ihrer Überprüfung bei der Einreise der Fluggäste nach Kanada und während ihres Aufenthalts in diesem Land auf neue Umstände gestützt werden musste, die eine solche Verwendung rechtfertigten [243], und klargestellt, dass, wenn „es objektive Anhaltspunkte dafür [gibt], dass die PNR-Daten eines oder mehrerer Fluggäste einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten oder grenzübergreifender schwerer Kriminalität leisten könnten, … die Verwendung der Daten nicht über das hinauszugehen [scheint], was absolut notwendig ist“ [244]. Unter entsprechendem Verweis auf Rn. 120 des Urteils Tele2 Sverige hat der Gerichtshof für Recht erkannt, dass, damit in der Praxis die vollständige

239 Vgl. u. a. Urteil La Quadrature du Net (Rn. 148 und 149).

240 Gleiches gilt für Anforderungen von PNR-Daten durch die PNR-Zentralstellen anderer Mitgliedstaaten gemäß Art. 9 Abs. 2 der PNR-Richtlinie.

241 Vgl. Gutachten 1/15 (Rn. 192 und die dort angeführte Rechtsprechung). Vgl. unlängst Urteile Privacy International (Rn. 77) und – entsprechend – Prokuratuur (Rn. 49 und die dort angeführte Rechtsprechung).

242 Vgl. Gutachten 1/15 (Rn. 200).

243 Vgl. Gutachten 1/15 (Rn. 200).

244 Vgl. Gutachten 1/15 (Rn. 201).

Einhaltung dieser Voraussetzungen gewährleistet ist, „es unabdingbar [ist], dass die Verwendung der gespeicherten PNR-Daten während des Aufenthalts der Fluggäste in Kanada grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und dass deren Entscheidung im Anschluss an einen mit Gründen versehenen Antrag ergeht, der von den zuständigen Behörden insbesondere im Rahmen von Verfahren zur Verhütung, Aufdeckung oder Verfolgung von Straftaten gestellt wird“ [245]. Der Gerichtshof hat die Möglichkeit einer Verwendung der nach ihrer Überprüfung anlässlich einer Flugreise gespeicherten PNR-Daten daher einer doppelten Voraussetzung unterworfen, die sowohl materiell-rechtlich – es müssen nämlich objektive Gründe vorliegen, die eine solche Verwendung rechtfertigen – als auch verfahrensrechtlich – nämlich die Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle – ist. Weit davon entfernt, „kontextbezogen“ zu sein, stellt die Auslegung durch den Gerichtshof die Anwendung der sich u. a. aus den Urteilen Digital Rights und Tele2 Sverige ergebenden Rechtsprechung im Bereich der PNR-Daten dar.

250. Das mit der PNR-Richtlinie während der ersten sechs Monate der Speicherung von PNR-Daten geschaffene System, das nach der in Art. 6 Abs. 2 Buchst. a dieser Richtlinie genannten Vorabüberprüfung eine potenziell wiederholte Übermittlung und Verarbeitung von PNR-Daten ohne angemessene Verfahrensgarantien sowie ohne hinreichend klare und präzise materiell-rechtliche Regeln gestattet, die den Gegenstand und die Modalitäten der verschiedenen Eingriffe definieren, genügt nicht den Anforderungen, die der Gerichtshof im Gutachten 1/15 aufgestellt hat. Es scheint auch nicht dem Erfordernis einer auf das absolut Notwendige beschränkten Verwendung der PNR-Daten zu genügen.

251. Ich schlage dem Gerichtshof daher vor, Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie in einer Weise auszulegen, dass Datenverarbeitungen nach dieser Vorschrift, die während der in Art. 12 Abs. 2 der Richtlinie vorgesehenen anfänglichen Frist von sechs Monaten erfolgen, den Anforderungen genügen, die der Gerichtshof im Gutachten 1/15 festgelegt hat.

252. Was die erste Voraussetzung materiell-rechtlicher Natur angeht, von der der Gerichtshof die weitere Nutzung der PNR-Daten abhängig gemacht hat, so können die Begriffe „berechtigter Grund“ im Sinne von Art. 12 Abs. 3 Buchst. a der PNR-Richtlinie und „hinreichende Grundlage“ gemäß deren Art. 6 Abs. 2 Buchst. b dieser Richtlinie meiner Ansicht nach ohne Weiteres dahin ausgelegt werden, dass in Anfragen der darin genannten zuständigen Behörden „objektive Anhaltspunkte dafür [angeführt werden müssen], dass die PNR-Daten eines oder mehrerer Fluggäste einen wirksamen Beitrag zur Bekämpfung terroristischer Straftaten oder … schwerer Kriminalität leisten könnten“ [246].

253. Was die zweite Voraussetzung verfahrensrechtlicher Natur betrifft, so ist Art. 6 Abs. 2 Buchst. b der PNR-Richtlinie in Verbindung mit deren Art. 12 Abs. 3 im Licht der Art. 7, 8 und 52 Abs. 1 der Charta nach meinem Dafürhalten dahin auszulegen, dass das in Art. 12 Abs. 3 Buchst. b dieser Richtlinie vorgesehene Erfordernis der vorherigen Genehmigung durch eine Justizbehörde oder eine unabhängige Verwaltungsstelle für jede Verarbeitung von PNR-Daten gemäß Art. 6 Abs. 2 Buchst. b gilt.

[245] Vgl. Gutachten 1/15 (Rn. 202).

[246] Vgl. in diesem Sinne Gutachten 1/15 (Rn. 201).

4. Ergebnisse zur zweiten, zur dritten, zur vierten, zur sechsten und zur achten Vorlagefrage

254. Nach alledem schlage ich dem Gerichtshof vor, Anhang I Nr. 12 insoweit für ungültig zu erklären, als in dieser Nummer „allgemeine Hinweise“ zu den Kategorien von PNR-Daten gezählt werden, die die Fluggesellschaften den PNR-Zentralstellen gemäß Art. 8 der PNR-Richtlinie zu übermitteln haben, und festzustellen, dass die Prüfung der zweiten, der dritten, der vierten, der sechsten und der achten Vorlagefrage vorbehaltlich der in den Nrn. 153, 160, 161 bis 164, 219, 228, 239 und 251 der vorliegenden Schlussanträge vorgeschlagenen Auslegungen dieser Richtlinie keine weiteren Anhaltspunkte ergeben hat, die geeignet sind, die Gültigkeit der Richtlinie zu beeinträchtigen.

255. Im Licht der Antwort, die ich auf die Vorlagefragen nach der Gültigkeit der PNR-Richtlinie zu geben vorschlage, kann dem u. a. vom Rat gestellten Antrag auf Aufrechterhaltung der Wirkungen dieser Richtlinie für den Fall, dass der Gerichtshof beschließen sollte, die Richtlinie insgesamt vollständig oder teilweise für ungültig zu erklären, unabhängig von anderen Erwägungen nicht stattgegeben werden.

C. Zur fünften Vorlagefrage

256. Mit seiner fünften Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof erfahren, ob Art. 6 der PNR-Richtlinie in Verbindung mit den Art. 7, 8 und 52 Abs. 1 der Charta dahin auszulegen ist, dass er einzelstaatlichen Rechtsvorschriften entgegensteht, die als Verarbeitungszweck der PNR-Daten die Beaufsichtigung bestimmter Aktivitäten der Nachrichten- und Sicherheitsdienste zulassen. Aus der Vorlageentscheidung geht hervor, dass es sich bei diesen Aktivitäten um die Tätigkeiten der Staatssicherheit sowie des Allgemeinen Nachrichten- und Sicherheitsdiensts im Rahmen ihres Auftrags im Zusammenhang mit dem Schutz der nationalen Sicherheit handelt.

257. Wie ich in den Nrn. 113 und 114 der vorliegenden Schlussanträge ausgeführt habe, ist die Abgrenzung der Zwecke der Verarbeitung personenbezogener Daten eine wesentliche Garantie, die es zu beachten gilt, damit Eingriffe in die in den Art. 7 und 8 der Charta niedergelegten Grundrechte nicht über das hinausgehen, was im Sinne der Rechtsprechung des Gerichtshofs notwendig ist. Ich habe ebenfalls bereits klargestellt, dass es, was in der PNR-Richtlinie vorgesehene Eingriffe in diese Grundrechte angeht, Sache des Unionsgesetzgebers war, klare und präzise Regeln für die Tragweite und die Anwendung der solche Eingriffe enthaltenden Maßnahmen vorzusehen, damit die u. a. in Art. 52 Abs. 1 der Charta verankerten Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit gewahrt werden.

258. In Art. 1 Abs. 2 der PNR-Richtlinie heißt es, dass die nach deren Maßgabe erhobenen PNR-Daten „ausschließlich zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gemäß Artikel 6 Absatz 2 Buchstaben a, b und c verarbeitet werden [dürfen]“. Nach dieser Vorschrift verarbeiten die PNR-Zentralstellen PNR-Daten ausschließlich mit dem Ziel, eine Vorabüberprüfung von Fluggästen vorzunehmen (Art. 6 Abs. 2 Buchst. a), punktuelle Anfragen zuständiger Behörden zu beantworten (Art. 6 Abs. 2 Buchst. b) und die Kriterien zu aktualisieren oder neue Kriterien zur Verwendung in gemäß Art. 6 Abs. 3 Buchst. b vorgenommenen Überprüfungen aufzustellen (Art. 6 Abs. 2 Buchst. c). In allen drei Fällen wird ausdrücklich auf die in Art. 1 Abs. 2 der PNR-Richtlinie angegebenen Ziele im Bereich der Bekämpfung von Terrorismus und schwerer Kriminalität hingewiesen.

259. Darüber hinaus stellt Art. 7 Abs. 4 der PNR-Richtlinie klar, dass nicht nur die in deren Art. 6 vorgesehene Verarbeitung von PNR-Daten, sondern auch die Weiterverarbeitung dieser Daten und der Verarbeitungsergebnisse durch die zuständigen Behörden der Mitgliedstaaten „ausschließlich [auf den] bestimmten Zweck der Verhütung, Aufdeckung, Ermittlung oder Verfolgung terroristischer Straftaten oder schwerer Kriminalität“ beschränkt werden müssen.

260. Der erschöpfende Charakter der Abgrenzung der mit der PNR-Richtlinie verfolgten Ziele geht eindeutig aus dem Wortlaut von Art. 1 Abs. 2 dieser Richtlinie hervor und wird außer durch deren Art. 6 Abs. 2 und Art. 7 Abs. 4, die bereits erwähnt worden sind, durch mehrere Artikel und Erwägungsgründe der Richtlinie untermauert, die jeden Verfahrensschritt beim Zugang, bei der Verarbeitung, bei der Speicherung und beim Teilen von PNR-Daten systematisch ausschließlich mit diesen spezifischen Zielen verknüpfen [247].

261. Sowohl aus dem Wortlaut von Art. 1 Abs. 2 der PNR-Richtlinie als auch aus seiner Auslegung im Licht der Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit, nach denen die Zwecke der Maßnahmen, die Eingriffe in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten enthalten, abschließend eingegrenzt werden müssen, ergibt sich, dass jede Ausweitung der Zwecke der Verarbeitung von PNR-Daten über die in dieser Vorschrift ausdrücklich erwähnten Sicherheitsziele hinaus gegen die PNR-Richtlinie verstößt.

262. Das Verbot einer Ausdehnung der mit der Richtlinie verfolgten Ziele gilt nach meinem Dafürhalten ganz besonders für die Tätigkeiten der Sicherheits- und Nachrichtendienste der Mitgliedstaaten, auch wegen des Mangels an Transparenz, der ihren *Modus operandi* kennzeichnet. Insoweit stimme ich mit der Kommission überein, nämlich dass diese Dienste in der Regel keinen direkten Zugang zu PNR-Daten haben sollten. In diesem Kontext halte ich bereits den Umstand an sich für fragwürdig, dass von den Sicherheitsdiensten abgeordnete Beamte zu den Mitgliedern der nationalen PNR-Zentralstellen zählen können, wie bei der belgischen PNR-Zentralstelle der Fall [248].

263. Auf der Grundlage der vorstehenden Erwägungen ist meiner Ansicht nach auf die fünfte Vorlagefrage zu antworten, dass die PNR-Richtlinie, insbesondere ihr Art. 1 Abs. 2 und ihr Art. 6, dahin auszulegen ist, dass sie einzelstaatlichen Rechtsvorschriften entgegensteht, die als Verarbeitungszweck der PNR-Daten die Beaufsichtigung bestimmter Aktivitäten der Nachrichten- und Sicherheitsdienste zulassen, soweit die nationale PNR-Zentralstelle im Rahmen eines solchen Zwecks gehalten wäre, die Daten zu verarbeiten und/oder sie oder die Ergebnisse ihrer Verarbeitung zu anderen als den in Art. 1 Abs. 2 dieser Richtlinie erschöpfend aufgeführten Zwecken an die erwähnten Dienste zu übermitteln, was das nationale Gericht zu prüfen hat.

[247] Vgl. u. a. Art. 4, Art. 7 Abs. 1 und 2, Art. 9 Abs. 2, Art. 10 Abs. 2 sowie Art. 12 Abs. 4 der PNR-Richtlinie; vgl. u. a. Erwägungsgründe 6, 9, 10, 11, 15, 23, 25, 35 und 38 dieser Richtlinie. Ich weise ferner darauf hin, dass es im 28. Erwägungsgrund des Vorschlags für eine PNR-Richtlinie hieß: „Die vorliegende Richtlinie hindert die Mitgliedstaaten nicht daran, … nach ihrem jeweiligen innerstaatlichen Recht … eine Regelung zur Erfassung und Verarbeitung von PNR-Daten für andere als mit dieser Richtlinie verfolgte Zwecke … vorzusehen.“ Die vorstehende Klarstellung ist jedoch nicht in die endgültige Fassung der PNR-Richtlinie übernommen worden.

[248] Die vorstehend beschriebene Möglichkeit ist jedoch gemäß Art. 4 Abs. 3 der PNR-Richtlinie, wonach „[d]as Personal der PNR-Zentralstelle aus Mitarbeitern zuständiger Behörden bestehen [kann], die zu diesem Zweck abgeordnet wurden“, zumindest insoweit zulässig, als die Nachrichten- und Sicherheitsdienste des betreffenden Mitgliedstaats als „zuständige Behörden“ im Sinne von Art. 7 Abs. 2 der PNR-Richtlinie eingestuft werden können.

D. Zur siebten Vorlagefrage

264. Mit seiner siebten Frage möchte das vorlegende Gericht vom Gerichtshof wissen, ob Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie dahin auszulegen ist, dass die PNR-Zentralstelle eine „zuständige nationale Behörde" im Sinne dieser Vorschrift darstellt, die nach Ablauf der anfänglichen Frist von sechs Monaten ab Übermittlung der PNR-Daten deren vollständige Offenlegung gestatten kann.

265. Art. 12 Abs. 2 der PNR-Richtlinie sieht vor, dass die PNR-Daten nach Ablauf einer Frist von sechs Monaten durch Unkenntlichmachung bestimmter Elemente, mit denen die Identität des Fluggasts, auf den sie sich beziehen, unmittelbar festgestellt werden könnte, depersonalisiert werden. Nach Fristablauf ist die Offenlegung der vollständigen PNR-Daten nur unter den in Art. 12 Abs. 3 vorgesehenen Voraussetzungen und insbesondere dann zulässig, wenn die Offenlegung zuvor genehmigt wird durch eine „Justizbehörde" (Art. 12 Abs. 3 Buchst. b Ziff. i) oder eine „andere nationale Behörde, die nach nationalem Recht dafür zuständig ist zu überprüfen, ob die Bedingungen für die Offenlegung erfüllt sind, vorbehaltlich der Unterrichtung des Datenschutzbeauftragten der PNR-Zentralstelle und einer Ex-Post-Überprüfung durch diesen Datenschutzbeauftragten" (Art. 12 Abs. 3 Buchst. b Ziff. ii).

266. Die meisten Regierungen, die im vorliegenden Verfahren schriftliche Erklärungen vorgelegt haben, haben sich nicht zur siebten Vorlagefrage geäußert. Die tschechische Regierung vertritt wie die Kommission die Auffassung, Art. 12 Abs. 3 der PNR-Richtlinie dürfe nicht dahin ausgelegt werden, dass die PNR-Zentralstelle eine „zuständige nationale Behörde" darstellen könne. Die belgische [249], die irische, die spanische, die französische und die zyprische Regierung treten einer solchen Auslegung jedoch entgegen. Sie gehen im Wesentlichen davon aus, dass keine Bestimmung der PNR-Richtlinie oder des Unionsrechts einer Benennung der PNR-Zentralstelle als zuständige nationale Behörde im Sinne von Art. 12 Abs. 2 Buchst. b Ziff. ii dieser Richtlinie entgegenstehe und die PNR-Zentralstelle naturgemäß eine hinreichend unabhängige Behörde sei, um die Verarbeitung der PNR-Daten genehmigen zu können.

267. Ich für meinen Teil stelle erstens fest, dass der Unionsgesetzgeber, wie aus dem Wortlaut von Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie, insbesondere aus der Verwendung der Konjunktion „oder", die die beiden Fallkonstellationen in den Ziff. i und ii dieser Vorschrift miteinander verbindet, hervorgeht, die Kontrolle durch die nationale Behörde nach Ziff. ii und die Kontrolle durch die Justizbehörde nach Ziff. i auf eine Stufe stellen wollte. Folglich muss die besagte nationale Behörde ein solches Maß an Unabhängigkeit und Unparteilichkeit aufweisen, dass die von ihr ausgeübte Kontrolle als eine Alternative anzusehen ist, die mit der Kontrolle, die von einer Justizbehörde vorgenommen werden kann, vergleichbar ist [250].

268. Zweitens ergibt sich aus den vorbereitenden Arbeiten zur PNR-Richtlinie, dass der Unionsgesetzgeber zum einen dem Vorschlag der Kommission, den Leiter der PNR-Zentralstelle mit der Aufgabe zu betrauen, die Offenlegung der vollständigen PNR-Daten zu genehmigen [251],

[249] Zu den Zweifeln der belgischen Regierung hinsichtlich der Zuständigkeit des Gerichtshofs für die Beantwortung der siebten Vorlagefrage ist zu sagen, dass das vorlegende Gericht den Gerichtshof ausweislich des Wortlauts der Frage zur Auslegung von Art. 12 Abs. 3 der PNR-Richtlinie und nicht zur Vereinbarkeit der nationalen Rechtsvorschriften mit dieser Vorschrift befragt. Jedenfalls kann der Gerichtshof den nationalen Gerichten nach ständiger Rechtsprechung Hinweise geben, die es ihnen ermöglichen, diese Unvereinbarkeit zu beurteilen (vgl. u. a. Urteil vom 7. September 2016, ANODE, C-121/15, EU:C:2016:637, Rn. 54 und die dort angeführte Rechtsprechung).

[250] Vgl. insoweit Urteil vom 5. November 2019, Kommission/Polen (Unabhängigkeit der ordentlichen Gerichte) (C-192/18, EU:C:2019:924, Rn. 108 bis 110).

[251] Art. 9 Abs. 2 Satz 4 des Vorschlags für eine PNR-Richtlinie bestimmte, dass „[d]er Zugriff auf die vollständigen PNR-Daten … vom Leiter der PNR-Zentralstelle genehmigt werden muss".

nicht gefolgt ist und zum anderen die von der Kommission vorgeschlagene anfängliche Frist für die Datenspeicherung, die sich auf 30 Tage belief, auf sechs Monate verlängert hat. In diesem Kontext, der durch das Bemühen um ein Gleichgewicht zwischen der Dauer der Speicherfrist vor der Depersonalisierung der PNR-Daten und den Voraussetzungen gekennzeichnet ist, denen ihre Unkenntlichmachung am Ende dieser Frist unterliegt, ist die Entscheidung des Unionsgesetzgebers zu sehen, den vollständigen Zugang zu den PNR-Daten strengeren verfahrensrechtlichen Bedingungen zu unterwerfen, als sie von der Kommission ursprünglich vorgesehen waren, und eine unabhängige Behörde mit der Überprüfung zu beauftragen, ob die Bedingungen für die Offenlegung erfüllt sind.

269. Drittens geht aus der Systematik der PNR-Richtlinie, wie die Kommission zu Recht festgestellt hat, hervor, dass die Daseinsberechtigung des in Art. 12 Abs. 3 der PNR-Richtlinie vorgesehenen Genehmigungsverfahrens darin liegt, eine unparteiische Drittpartei mit der Aufgabe zu betrauen, in jedem Einzelfall eine Abwägung der Rechte der betroffenen Personen mit dem Strafverfolgungszweck vorzunehmen, der mit dieser Richtlinie verfolgt wird.

270. Viertens ergibt sich aus der Rechtsprechung des Gerichtshofs, dass eine Stelle, die mit der Durchführung der vorherigen Kontrolle betraut ist, der es bedarf, um den Zugang der zuständigen nationalen Behörden zu rechtmäßig gespeicherten personenbezogenen Daten zu genehmigen, über alle Befugnisse verfügen und alle Garantien aufweisen muss, die erforderlich sind, um zu gewährleisten, dass die verschiedenen einander gegenüberstehenden Interessen und Rechte in Einklang gebracht werden. Der Gerichtshof hat darüber hinaus klargestellt, dass diese Stelle über eine Stellung verfügen muss, die es ihr erlaubt, bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorzugehen, ohne jede Einflussnahme von außen [252]. In Anbetracht des Erfordernisses der Unabhängigkeit muss es sich bei der mit der vorherigen Kontrolle betrauten Behörde – vor allem im strafrechtlichen Bereich – insbesondere um eine andere als die den Zugang zu den Daten begehrende Stelle handeln, so dass sie nicht an der Durchführung eines Ermittlungsverfahrens beteiligt sein darf und eine Position der Neutralität gegenüber den Beteiligten am Strafverfahren bewahren muss [253].

271. Festzustellen ist, dass die PNR-Zentralstelle nicht alle Garantien der Unabhängigkeit und Unparteilichkeit aufweist, denen die mit der Wahrnehmung der in Art. 12 Abs. 3 der PNR-Richtlinie vorgesehenen vorherigen Kontrolle betraute Behörde genügen muss. Die PNR-Zentralstellen sind nämlich unmittelbar mit den für die Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität zuständigen Behörden verbunden. Nach Art. 4 Abs. 1 der PNR-Richtlinie ist die PNR-Zentralstelle selbst eine solche Behörde oder eine Abteilung einer solchen Behörde. Darüber hinaus sieht Art. 4 Abs. 3 vor, dass das Personal der PNR-Zentralstelle aus Mitarbeitern zuständiger Behörden bestehen kann, die zu diesem Zweck abgeordnet wurden. Das ist u. a. bei der belgischen PNR-Zentralstelle der Fall, deren Mitglieder gemäß Art. 14 des PNR-Gesetzes u. a. von den Polizeidiensten, der Staatssicherheit, dem Allgemeinen Nachrichten- und Sicherheitsdienst sowie der Generalverwaltung Zoll und Akzisen entsandt werden.

272. Zwar müssen die Mitglieder der PNR-Zentralstelle allgemein Gewähr für Integrität, Befähigung, Transparenz und Unabhängigkeit bieten und haben die Mitgliedstaaten gegebenenfalls dafür Sorge zu tragen, dass diese Garantien unter Berücksichtigung der Verbindungen zu ihren Mitgliedskörperschaften konkret gewahrt werden können, damit insbesondere gewährleistet ist, dass die zuständigen Behörden, in deren Aufbau die Mitglieder

252 Urteil Prokuratuur (Rn. 52 und 53).

253 Urteil Prokuratuur (Rn. 53 und 54). Vgl. in demselben Sinne Urteil Big Brother Watch (§§ 349 bis 352).

originär eingefügt sind, einen direkten Zugang zur PNR-Datenbank haben und nicht nur zu den Ergebnissen der von den PNR-Zentralstellen vorgenommenen Eingaben. Gleichwohl haben die Mitglieder der PNR-Zentralstellen, die von zuständigen Behörden im Sinne von Art. 7 Abs. 2 der PNR-Richtlinie entsandt werden, während des Zeitraums ihrer Entsendung weiterhin unweigerlich eine Bindung zu ihren ursprünglichen Diensten, da sie ihr Statut behalten, auch wenn sie der funktionellen und hierarchischen Amtsgewalt des leitenden Beamten der PNR-Zentralstelle unterstellt werden.

273. Die Schlussfolgerung, wonach die PNR-Zentralstelle keine nationale Behörde im Sinne von Art. 12 Abs. 3 Buchst. b Ziff. ii der PNR-Richtlinie ist, wird darüber hinaus durch den Umstand untermauert, dass der Datenschutzbeauftragte der betreffenden PNR-Zentralstelle nach dieser Vorschrift über den Offenlegungsantrag „unterrichtet" werden muss und eine „Ex-Post-Überprüfung" vornimmt. Wäre die PNR-Zentralstelle nämlich als „andere nationale Behörde" befugt, einem Offenlegungsantrag gemäß Art. 12 Abs. 3 der PNR-Richtlinie stattzugeben, würde der Datenschutzbeauftragte, der nach Art. 5 Abs. 1 dieser Richtlinie u. a. für die Umsetzung der maßgeblichen Sicherheitsvorkehrungen bei der Verarbeitung der PNR-Daten zuständig ist, zum Zeitpunkt der Stellung des Zugangsantrags unterrichtet, so dass seine Kontrolle notwendigerweise *ex ante* erfolgen würde [254].

274. Im Licht der vorstehenden Erwägungen schlage ich dem Gerichtshof vor, auf die siebte Vorlagefrage zu antworten, dass Art. 12 Abs. 3 Buchst. b der PNR-Richtlinie dahin auszulegen ist, dass die PNR-Zentralstelle keine „andere zuständige nationale Behörde" im Sinne dieser Vorschrift darstellt.

E. Zur neunten Vorlagefrage

275. Mit seiner neunten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof zum einen erfahren, ob die API-Richtlinie mit Art. 3 Abs. 2 EUV und mit Art. 45 der Charta vereinbar ist, insofern sie für Flüge innerhalb der Union gilt, und zum anderen, ob diese Richtlinie in Verbindung mit Art. 3 Abs. 2 EUV und mit Art. 45 der Charta dahin auszulegen ist, dass sie einzelstaatlichen Rechtsvorschriften entgegensteht, die zum Zwecke der Bekämpfung der illegalen Einwanderung und der Verbesserung der Grenzkontrollen ein System zur Erhebung und Verarbeitung der Daten zu den beförderten Passagieren gestatten, das indirekt eine Wiedereinführung von Kontrollen an den Binnengrenzen bedeuten könnte.

276. Aus der Vorlageentscheidung geht hervor, dass sich die Vorlagefrage in den Rahmen der Prüfung des zweiten Klagegrundes einfügt, den die LDH hilfsweise vorgebracht hat. Dieser Klagegrund, mit dem ein Verstoß gegen Art. 22 der belgischen Verfassung in Verbindung mit Art. 3 Abs. 2 EUV und mit Art. 45 der Charta geltend gemacht wird, richtet sich gegen Art. 3 § 1, Art. 8 § 2 und Kapitel 11, insbesondere dessen Art. 28 bis 31, des PNR-Gesetzes. Während der erstgenannte Artikel allgemein den Gegenstand dieses Gesetzes festlegt, indem er klarstellt, dass es „die Verpflichtungen der Beförderungsunternehmen und Reiseunternehmen in Bezug auf die Übermittlung von Daten zu Passagieren, die in das nationale Hoheitsgebiet, aus dem nationalen Hoheitsgebiet oder durch das nationale Hoheitsgebiet befördert werden[, bestimmt]", sieht Art. 8 § 2 des Gesetzes vor, dass „[d]ie Passagierdaten … unter den in [dessen] Kapitel 11 erwähnten Bedingungen ebenfalls verarbeitet [werden], um die Personenkontrolle an den Außengrenzen zu verbessern und die illegale Einwanderung zu bekämpfen". Im Rahmen dieses

[254] Art. 9 Abs. 2 Satz 4 des Vorschlags für eine PNR-Richtlinie bestimmte, dass „[d]er Zugriff auf die vollständigen PNR-Daten … vom Leiter der PNR-Zentralstelle genehmigt werden muss".

Zwecks werden den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt (Belgien) nach Art. 29 § 1 des PNR-Gesetzes nur die in dessen Art. 9 § 1 Nr. 18 erwähnten „Passagierdaten“ (nämlich die in Anhang I Nr. 18 der PNR-Richtlinie genannten API-Daten) in Bezug auf drei Kategorien von Passagieren übermittelt. Dabei handelt es sich um „Passagiere, die beabsichtigen, über die Außengrenzen Belgiens ins Hoheitsgebiet zu kommen, oder bereits über die Außengrenzen Belgiens ins Hoheitsgebiet gekommen sind“, „Passagiere, die beabsichtigen, das Hoheitsgebiet über die Außengrenzen Belgiens zu verlassen, oder die das Hoheitsgebiet bereits über die Außengrenzen Belgiens verlassen haben“, und „Passagiere, die beabsichtigen, sich in einer in Belgien gelegenen internationalen Transitzone aufzuhalten, sich dort aufhalten oder sich dort aufgehalten haben“ [255]. Aus Art. 29 § 3 des PNR-Gesetzes geht hervor, dass diese Daten den Polizeidiensten, die mit der Grenzkontrolle beauftragt sind, und dem Ausländeramt von der PNR-Zentralstelle „unmittelbar nach ihrer Speicherung in der Passagierdatenbank“ übermittelt und innerhalb von 24 Stunden nach ihrer Übermittlung vernichtet werden. Nach § 4 kann, wenn der Zugriff auf die Daten nach Ablauf dieser Frist noch notwendig ist, damit das Ausländeramt seinen gesetzlichen Auftrag ausführen kann, auch das Ausländeramt eine gebührend mit Gründen versehene Anfrage an die PNR-Zentralstelle richten. Daher verlässt der rechtliche Rahmen, in den sich die neunte Vorlagefrage einfügt, angesichts des Zwecks der in den Art. 28 und 29 des PNR-Gesetzes genannten Datenverarbeitung den rechtlichen Rahmen der PNR-Richtlinie und fügt sich in denjenigen der API-Richtlinie ein. Darüber hinaus geht aus den bei der Kanzlei des Gerichtshofs eingereichten Akten u. a. hervor, dass der zweite Klagegrund der LDH auf einer Auslegung der Bestimmungen von Kapitel 11 des PNR-Gesetzes beruht, wonach diese auch im Fall einer Überschreitung der Binnengrenzen Belgiens gelten.

277. Der erste Teil der neunten Vorlagefrage beruht auf einer falschen Annahme und bedarf nach meinem Dafürhalten keiner Antwort des Gerichtshofs. Aus Art. 3 Abs. 1 der API-Richtlinie in Verbindung mit deren Art. 2 Buchst. b und d geht nämlich eindeutig hervor, dass diese Richtlinie die Fluggesellschaften verpflichtet, den mit der Durchführung der Personenkontrollen an den Außengrenzen beauftragten Behörden die API-Daten nur in Bezug auf Flüge zu übermitteln, mit denen beförderte Personen zu einem für die Überschreitung der Außengrenzen der Mitgliedstaaten zu Drittstaaten zugelassenen Übergang verbracht werden. Desgleichen sieht Art. 6 Abs. 1 der Richtlinie nur die Verarbeitung der API-Daten zu diesen Flügen vor. Im Übrigen haben die Mitgliedstaaten nach der PNR-Richtlinie zwar die Möglichkeit, die Verpflichtung zur Übermittlung erhobener API-Daten auch auf Fluggesellschaften auszudehnen, die EU-Flüge durchführen, diese Ausdehnung muss aber die API-Richtlinie unberührt lassen [256]. Im Rahmen der PNR-Richtlinie werden die übermittelten API-Daten nur im Rahmen der in dieser Richtlinie vorgesehenen Strafverfolgungszwecke verarbeitet. Umgekehrt sieht der 34. Erwägungsgrund der PNR-Richtlinie vor, dass diese gegenwärtige Regelungen der Union hinsichtlich der Durchführung von Grenzkontrollen und Regelungen der Union hinsichtlich der Einreise in das Gebiet der Union und der Ausreise aus dem Gebiet der Union unberührt lässt, und Art. 6 Abs. 9 Satz 2 der Richtlinie bestimmt, dass, wenn Überprüfungen nach Abs. 2 in Bezug auf EU-Flüge zwischen Mitgliedstaaten vorgenommen werden, für die der Schengener Grenzkodex [257] gilt, die Auswirkungen solcher Überprüfungen mit diesem im Einklang stehen müssen.

278. Würde der erste Teil der neunten Vorlagefrage, wie die Kommission hilfsweise vorschlägt, dahin gehend umformuliert, dass er sich nicht auf die Vereinbarkeit der API-Richtlinie mit den Bestimmungen des Vertrags und der Charta, sondern auf die Frage bezieht, ob die

255 Art. 29 §§ 1 und 2 des PNR-Gesetzes.

256 Vgl. zehnter Erwägungsgrund der PNR-Richtlinie.

257 Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Unionskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. 2016, L 77, S. 1, im Folgenden: Schengener Grenzkodex).

PNR-Richtlinie, insbesondere ihr Art. 2, mit diesen Bestimmungen vereinbar ist, würde das nicht nur eine Änderung des Rechtsakts, in Bezug auf den das vorlegende Gericht um eine Beurteilung der Gültigkeit ersucht hat, sondern auch ein Verlassen des rechtlichen Rahmens bedeuten, in den sich die Vorlagefrage einfügt. Denn wie ich erläutert habe, wird mit den Bestimmungen von Kapitel 11 des PNR-Gesetzes, gegen die sich der zweite Klagegrund richtet, die API-Richtlinie und nicht die PNR-Richtlinie umgesetzt.

279. Für den Fall, dass der Gerichtshof eine solche Umformulierung vornimmt, beschränke ich mich auf einige Überlegungen, die sich insbesondere auf die Frage beziehen, ob die Vorabüberprüfung der PNR-Daten der Fluggäste von EU-Flügen, zu deren Durchführung die Mitgliedstaaten entsprechend der Befugnis berechtigt sind, über die sie im Sinne von Art. 2 der PNR-Richtlinie verfügen, der Durchführung von „Grenzübertrittskontrollen" im Sinne von Art. 23 Buchst. a des Schengener Grenzkodex gleichgestellt werden dürfen [258]. Erstens wird die Vorabüberprüfung der PNR-Daten, auch wenn sie nicht an der „Grenzübergangsstelle" oder zum „Zeitpunkt des Überschreitens der Grenze", sondern vor diesem Zeitpunkt erfolgt, gleichwohl „wegen" des bevorstehenden Überschreitens der Grenzen vorgenommen. Zweitens sind die Mitgliedstaaten nach Art. 2 der PNR-Richtlinie befugt, die in Art. 6 Abs. 2 Buchst. a dieser Richtlinie vorgesehene Vorabüberprüfung der PNR-Daten auf Fluggäste aller EU-Flüge auszudehnen, unabhängig vom Verhalten der betreffenden Personen oder von Umständen, aus denen sich die Gefahr einer Beeinträchtigung der öffentlichen Sicherheit ergibt. Die Vorabüberprüfung hat außerdem systematischen Charakter. Keiner der vorstehenden Gesichtspunkte scheint jedoch den in Art. 23 Buchst. a Satz 2 Ziff. ii, iii und iv des Schengener Grenzkodex genannten Anhaltspunkten zu genügen [259]. Drittens frage ich mich in Bezug auf die in Art. 23 Buchst. a Satz 2 Ziff. i und iii genannten Anhaltspunkte, ob sich die Vorabüberprüfung nach Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie nicht zumindest teilweise mit dem Zweck der Grenzübertrittskontrollen gemäß Art. 8 Abs. 2 Buchst. b sowie Art. 3 Buchst. a Ziff. vi und Buchst. g Ziff. iii des Schengener Grenzkodex in der durch die Verordnung 2017/458 geänderten Fassung deckt, und vor allem, ob sie sich hinsichtlich ihrer Modalitäten klar von diesen systematischen Kontrollen unterscheidet [260]. Ich stelle insoweit fest, dass die Abfragen, wie es in Art. 8 Abs. 2e und Abs. 3 Buchst. ia des Schengener Grenzkodex heißt, „im Voraus auf der Grundlage von Angaben über die beförderten Personen durchgeführt werden [können], die im Einklang mit der [API-Richtlinie] oder mit anderen Unions- oder nationalen Rechtsvorschriften übermittelt wurden". Allerdings ist es richtig, dass der Zweck der PNR-Richtlinie nicht darin besteht, „sich zu vergewissern, dass die betreffenden Personen in das Hoheitsgebiet des Mitgliedstaats einreisen oder aus ihm ausreisen *dürfen*", oder darin, „diese Personen daran [zu] hindern …, sich den [Kontrollen] zu entziehen", die der Gerichtshof als Ziele der „Grenzübertrittskontrollen" gemäß dem Schengener Grenzkodex anerkannt hat [261], da die Richtlinie ausschließlich Strafverfolgungszwecken dient. Zudem sieht Art. 23 Buchst. a Satz 2 Ziff. ii dieses Kodex ausdrücklich vor, dass die Ausübung polizeilicher Befugnisse dann nicht der

[258] Art. 23 Buchst. a des Schengener Grenzkodex sieht vor, dass die Ausübung der polizeilichen Befugnisse nicht der Durchführung von Grenzübertrittskontrollen gleichgestellt werden darf, wenn die polizeilichen Maßnahmen „i) keine Grenzkontrollen zum Ziel haben; ii) auf allgemeinen polizeilichen Informationen und Erfahrungen in Bezug auf mögliche Bedrohungen der öffentlichen Sicherheit beruhen und insbesondere auf die Bekämpfung der grenzüberschreitenden Kriminalität abzielen; iii) in einer Weise konzipiert sind und durchgeführt werden, die sich eindeutig von systematischen Personenkontrollen an den Außengrenzen unterscheidet; iv) auf der Grundlage von Stichproben durchgeführt werden".

[259] Vgl. entsprechend Urteil vom 13. Dezember 2018, Touring Tours und Travel und Sociedad de transportes (C-412/17 und C-474/17, EU:C:2018:1005, Rn. 61 und die dort angeführte Rechtsprechung), sowie Beschluss vom 4. Juni 2020, FU (C-554/19, nicht veröffentlicht, EU:C:2020:439, Rn. 49 bis 56).

[260] Der Gerichtshof hat in Rn. 188 des Gutachtens 1/15 insoweit festgestellt, dass „die Identifizierung von Fluggästen, von denen ein Risiko für die öffentliche Sicherheit ausgehen kann, anhand der PNR-Daten zur Grenzkontrolle [gehört]".

[261] Vgl. Urteil vom 13. Dezember 2018, Touring Tours und Travel und Sociedad de transportes (C-412/17 und C-474/17, EU:C:2018:1005, Rn. 55 und die dort angeführte Rechtsprechung).

Durchführung von Grenzübertrittskontrollen gleichgestellt werden kann, wenn die Kontrollen u. a. auf die Bekämpfung der grenzüberschreitenden Kriminalität abzielen [262]. Schließlich sollte der Gerichtshof in seiner Beurteilung auch den u. a. von der Kommission hervorgehobenen Umstand berücksichtigen, dass Art. 2 der PNR-Richtlinie den Mitgliedstaaten nur gestattet, die Fluggesellschaften zur Übermittlung der von ihnen im Rahmen ihrer normalen Geschäftstätigkeit erhobenen PNR-Daten zu verpflichten, und daher keine Verpflichtung vorsieht, die der in der API-Richtlinie für die Überschreitung der Außengrenzen vorgesehenen Verpflichtung ähnelt.

280. Der zweite Teil der neunten Vorlagefrage ist meiner Ansicht nach – der Kommission folgend – so zu verstehen, dass er sich auf die Überschreitung der Binnengrenzen bezieht und mit ihm Klarstellungen vom Gerichtshof begehrt werden, die es dem vorlegenden Gericht ermöglichen, die Vereinbarkeit der Bestimmungen von Kapitel 11 des PNR-Gesetzes mit der Abschaffung der Kontrollen an den Binnengrenzen der Mitgliedstaaten im Schengen-Raum zu beurteilen.

281. Unter Berücksichtigung der spärlichen Informationen, über die der Gerichtshof verfügt, beschränke ich mich insoweit auf die Feststellung, dass die Bestimmungen von Kapitel 11 des PNR-Gesetzes nur mit dem Unionsrecht, insbesondere mit Art. 67 Abs. 2 AEUV, vereinbar sein können, wenn sie dahin ausgelegt werden, dass sie sich lediglich auf die Übermittlung und Verarbeitung der API-Daten von Fluggästen beziehen, die die Außengrenzen Belgiens zu Drittstaaten überschreiten.

282. Sollte der Gerichtshof beschließen, den zweiten Teil der neunten Vorlagefrage dahin gehend umzuformulieren, dass er sich auf die Auslegung der PNR-Richtlinie in Verbindung mit den Bestimmungen von Kapitel 11 des PNR-Gesetzes bezieht, beschränke ich mich auf die Feststellung, dass die in den Art. 28 und 29 dieses Gesetzes vorgesehene Verarbeitung von API-Daten das vom belgischen Gesetzgeber zur Umsetzung der PNR-Richtlinie geschaffene System überlagert. So handelt es sich erstens bei den API-Daten, die Gegenstand der Verarbeitung sind, um die in Anhang I Nr. 12 der PNR-Richtlinie aufgeführten und nicht lediglich um die Daten, die in der Liste in Art. 3 Abs. 2 der API-Richtlinie enthalten sind. Zweitens werden den mit der Grenzkontrolle beauftragten Polizeidiensten und dem Ausländeramt diese Daten nach Art. 29 § 1 des PNR-Gesetzes von der PNR-Zentralstelle – die nur für die Erhebung und Verarbeitung im Rahmen der mit der PNR-Richtlinie verfolgten Zwecke zuständig ist – und nicht, wie in der API-Richtlinie vorgesehen, unmittelbar von den Fluggesellschaften übermittelt. Darüber hinaus betrifft die Übermittlung auch Daten von Fluggästen, die beabsichtigen, das belgische Hoheitsgebiet zu verlassen, oder die das belgische Hoheitsgebiet bereits verlassen haben, und erfolgt nicht nur an die mit den Grenzkontrollen beauftragten Behörden, sondern auch an das Ausländeramt, das für die Steuerung der zugewanderten Bevölkerung und die Bekämpfung der illegalen Einwanderung zuständig ist. Drittens ist das Ausländeramt gemäß Art. 29 § 4 Abs. 2 des PNR-Gesetzes anscheinend befugt, Anträge auf Zugang zu API-Daten sogar nach Verarbeitung dieser Daten anlässlich des Grenzübertritts der betreffenden Fluggäste an die PNR-Zentralstelle zu richten. In diesem Sinne wird das Ausländeramt *de facto* einer zuständigen Behörde gemäß Art. 7 der PNR-Richtlinie gleichgestellt, obwohl sie anderer Natur und auch nicht auf der Liste mit zuständigen Behörden aufgeführt ist, die Belgien der Kommission übermittelt hat. Eine solche Vermengung der in der API- und in der PNR-Richtlinie

[262] Vgl. in diesem Sinne u. a. Beschluss vom 4. Juni 2020, FU (C-554/19, nicht veröffentlicht, EU:C:2020:439, Rn. 46).

vorgesehenen Systeme kann nach meinem Dafürhalten nicht hingenommen werden, da sie gegen den in Art. 1 Abs. 2 der PNR-Richtlinie verankerten Grundsatz der Zweckbindung verstößt [263].

283. Nach alledem schlage ich dem Gerichtshof vor, auf die neunte Vorlagefrage zu antworten, dass Art. 3 Abs. 1 der API-Richtlinie, wonach die Mitgliedstaaten die erforderlichen Schritte unternehmen, um die Fluggesellschaften zu verpflichten, auf Anfrage der mit der Durchführung der Personenkontrollen an den Außengrenzen beauftragten Behörden bei Abschluss des Check-in die Angaben über die in Abs. 2 in Verbindung mit Art. 2 Buchst. b und d dieser Richtlinie genannten Personen zu übermitteln, nur Personen betrifft, die zu einer für das Überschreiten der Außengrenzen der Mitgliedstaaten zu Drittstaaten zugelassenen Grenzübergangsstelle befördert werden. Einzelstaatliche Rechtsvorschriften, die diese Verpflichtung mit dem alleinigen Ziel der Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung auf die Daten von Personen ausdehnen würden, die mit dem Flugzeug oder mit anderen Verkehrsmitteln die Binnengrenzen des betreffenden Mitgliedstaats überschreiten, würden gegen Art. 67 Abs. 2 AEUV und Art. 22 des Schengener Grenzkodex verstoßen.

F. Zur zehnten Vorlagefrage

284. Mit seiner zehnten Vorlagefrage möchte das vorlegende Gericht vom Gerichtshof wissen, ob es, falls es zu dem Schluss gelangen sollte, dass das PNR-Gesetz gegen die Art. 7, 8 und 52 Abs. 1 der Charta verstößt, die Folgen dieses Gesetzes vorläufig aufrechterhalten könnte, um eine Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor gesammelten und auf Vorrat gespeicherten Daten noch für die durch das PNR-Gesetz angestrebten Ziele benutzt werden können.

285. Im Urteil La Quadrature du Net betreffend die Speicherung von Metadaten elektronischer Kommunikationen, das nach Einreichung des vorliegenden Vorabentscheidungsersuchens verkündet worden ist, hat der Gerichtshof auf eine gleichlautende Frage geantwortet. In diesem Urteil hat der Gerichtshof zunächst seine Rechtsprechung in Erinnerung gerufen, wonach der Vorrang und die einheitliche Anwendung des Unionsrechts beeinträchtigt würden, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen. Sodann hat er darauf hingewiesen, dass, wie er im Urteil vom 29. Juli 2019, Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen [264], in dem es um die Rechtmäßigkeit von Maßnahmen ging, die unter Verstoß gegen die durch das Unionsrecht auferlegte Pflicht zur Durchführung einer vorherigen Prüfung der Umweltverträglichkeit eines Projekts und seiner Verträglichkeit mit einem geschützten Gebiet ergangen waren, anerkannt hatte, ein nationales Gericht, wenn das innerstaatliche Recht es gestattet, die Wirkungen solcher Maßnahmen ausnahmsweise aufrechterhalten kann, sofern dies durch zwingende Erwägungen gerechtfertigt ist, die im Zusammenhang mit der Notwendigkeit stehen, die tatsächliche und schwerwiegende Gefahr einer Unterbrechung der Stromversorgung im betreffenden Mitgliedstaat für den Zeitraum abzuwenden, der absolut notwendig ist, um die Rechtswidrigkeit zu beseitigen. Er hat gleichwohl festgestellt, dass ein Verstoß gegen die in den Art. 7 und 8 der Charta garantierten Grundrechte im Gegensatz zu dem Versäumnis, einer prozeduralen Pflicht wie der vorherigen Prüfung der Auswirkungen eines Projekts im speziellen Bereich des Umweltschutzes nachzukommen, nicht

[263] Auch in ihrem Arbeitspapier von 2020 zur API-Richtlinie (S. 20) unterstreicht die Kommission den problematischen Charakter einer Überlagerung der Systeme zur Verarbeitung von PNR- und API-Daten auf nationaler Ebene.

[264] C-411/17, EU:C:2019:622 (Rn. 175, 176, 179 und 181).

durch ein Verfahren wie das im vorerwähnten Urteil vorgesehene geheilt werden kann [265]. Nach meinem Dafürhalten muss im vorliegenden Verfahren die gleiche Antwort auf die zehnte Vorlagefrage gegeben werden.

286. Soweit sowohl das vorlegende Gericht als auch die belgische Regierung sowie die Kommission und der Rat Bedenken hinsichtlich der Frage haben, ob das Unionsrecht einer Verwertung von Auskünften oder Beweisen im Rahmen eines Strafverfahrens entgegensteht, die unter Verwendung unionsrechtswidrig erhobener, verarbeiteter und/oder auf Vorrat gespeicherter PNR-Daten erlangt worden sind, weise ich darauf hin, dass es, wie der Gerichtshof in Rn. 222 des Urteils La Quadrature du Net klargestellt hat, beim gegenwärtigen Stand des Unionsrechts grundsätzlich allein Sache des nationalen Rechts ist, die Vorschriften für die Zulässigkeit und die Würdigung der durch eine solche unionsrechtswidrige Vorratsdatenspeicherung erlangten Informationen und Beweise im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, schwere Straftaten begangen zu haben, festzulegen, vorbehaltlich der Wahrung des Äquivalenz- und des Effektivitätsgrundsatzes. In Bezug auf Letzteren hat der Gerichtshof entschieden, dass der Effektivitätsgrundsatz ein nationales Strafgericht dazu verpflichtet, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen. Auch diese Grundsätze sind sinngemäß auf die Umstände des Ausgangsverfahrens übertragbar.

IV. Ergebnis

287. Nach alledem schlage ich dem Gerichtshof vor, auf die Vorlagefragen des Verfassungsgerichtshofs (Belgien) wie folgt zu antworten:

1. Art. 23 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) in Verbindung mit Art. 2 Abs. 2 Buchst. d dieser Verordnung ist dahin auszulegen, dass er

   – für nationale Rechtsvorschriften zur Umsetzung der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität gilt, soweit diese Rechtsvorschriften Verarbeitungen von PNR-Daten durch Fluggesellschaften und andere Wirtschaftsteilnehmer, einschließlich der in Art. 8 der Richtlinie vorgesehenen Übermittlung von PNR-Daten an die in deren Art. 4 genannten PNR-Zentralstellen, regeln;

   – nicht für nationale Rechtsvorschriften zur Umsetzung der Richtlinie 2016/681 gilt, soweit diese Rechtsvorschriften Datenverarbeitungen durch die zuständigen nationalen Behörden, einschließlich der PNR-Zentralstellen und gegebenenfalls der Sicherheits- und

[265] Vgl. Urteil La Quadrature du Net (Rn. 217 bis 219).

Nachrichtendienste des betreffenden Mitgliedstaats, zu den in Art. 1 Abs. 2 der Richtlinie vorgesehenen Zwecken regeln;

– für nationale Rechtsvorschriften zur Verbesserung der Personenkontrollen an den Außengrenzen und zur Bekämpfung der illegalen Einwanderung gilt, mit denen die Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, sowie die Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG umgesetzt werden.

2. Anhang I Nr. 12 der Richtlinie 2016/681 ist ungültig, soweit in dieser Nummer „allgemeine Hinweise“ zu den Datenkategorien gezählt werden, die die Fluggesellschaften den PNR-Zentralstellen gemäß Art. 8 der Richtlinie zu übermitteln haben.

3. Die Prüfung der zweiten, der dritten, der vierten, der sechsten und der achten Frage hat keine weiteren Anhaltspunkte ergeben, die geeignet sind, die Gültigkeit der Richtlinie 2016/681 zu beeinträchtigen.

4. Anhang I Nr. 12 der Richtlinie 2016/681 ist hinsichtlich des Teils, der nicht für ungültig erklärt wird, dahin auszulegen, dass diese Nummer nur Angaben zu Minderjährigen umfasst, die darin ausdrücklich erwähnt werden und unmittelbar mit dem Flug zusammenhängen.

5. Anhang I Nr. 18 der Richtlinie 2016/681 ist dahin auszulegen, dass diese Nummer nur darin sowie in Art. 3 Abs. 2 der Richtlinie 2004/82 ausdrücklich aufgeführte Vorabinformationen über Fluggäste umfasst, die von den Fluggesellschaften im Rahmen ihrer normalen Geschäftstätigkeit erhoben worden sind.

6. Der in Art. 6 Abs. 3 Buchst. a der Richtlinie 2016/681 genannte Begriff „maßgebliche Datenbanken“ ist dahin auszulegen, dass er sich nur auf nationale Datenbanken, die von den zuständigen Behörden gemäß Art. 7 Abs. 1 dieser Richtlinie verwaltet werden, sowie auf Datenbanken der Union und internationale Datenbanken bezieht, die von den zuständigen Behörden im Rahmen ihres Auftrags direkt betrieben werden. Die Datenbanken müssen in einem direkten und engen Zusammenhang mit den von der Richtlinie verfolgten Zwecken der Bekämpfung von Terrorismus und schwerer Kriminalität stehen, was voraussetzt, dass sie zu diesen Zwecken entwickelt worden sind. Im Rahmen der Umsetzung der Richtlinie 2016/681 in ihr nationales Recht sind die Mitgliedstaaten verpflichtet, eine Liste mit den entsprechenden Datenbanken zu veröffentlichen und auf dem neuesten Stand zu halten.

7. Art. 6 Abs. 3 Buchst. b der Richtlinie 2016/681 ist dahin auszulegen, dass er im Rahmen der darin vorgesehenen automatisierten Verarbeitung einer Verwendung algorithmischer Systeme entgegensteht, die ohne menschlichen Eingriff zu einer Änderung der im Voraus festgelegten Kriterien führen können, auf deren Grundlage diese Verarbeitung erfolgt ist und mit denen sich die Gründe, die zu einem Treffer bei der Verarbeitung geführt haben, nicht klar und transparent ermitteln lassen.

8. Art. 12 Abs. 1 der Richtlinie 2016/681 ist im Einklang mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass das Vorhalten der von den Fluggesellschaften an die PNR-Zentralstelle übermittelten PNR-Daten in einer Datenbank für einen Zeitraum von fünf Jahren ab ihrer Übermittlung an die PNR-Zentralstelle des Mitgliedstaats, in dessen Hoheitsgebiet der Flug angekommen bzw. von dem er abgegangen ist, nach Durchführung der Vorabüberprüfung gemäß Art. 6 Abs. 2 Buchst. a der PNR-Richtlinie nur insoweit zulässig ist, als auf der Grundlage objektiver Kriterien ein Zusammenhang zwischen diesen Daten und der Bekämpfung des Terrorismus oder schwerer Kriminalität festgestellt wird. Eine allgemeine und unterschiedslose Vorratsspeicherung von PNR-Daten in nicht anonymisierter Form lässt sich nur bei einer schwerwiegenden Gefahr für die Sicherheit der Mitgliedstaaten rechtfertigen, die sich als tatsächlich und gegenwärtig oder vorhersehbar erweist und beispielsweise mit terroristischen Handlungen zusammenhängt, sofern die Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt wird.

9. Art. 6 Abs. 2 Buchst. b der Richtlinie 2016/681 ist dahin auszulegen, dass eine Zurverfügungstellung von PNR-Daten oder der Ergebnisse der Datenverarbeitung nach dieser Vorschrift, die während der in Art. 12 Abs. 2 der Richtlinie vorgesehenen anfänglichen Frist von sechs Monaten erfolgt, die in Art. 12 Abs. 3 Buchst. b genannten Bedingungen erfüllen muss.

10. Die Richtlinie 2016/681, insbesondere ihr Art. 1 Abs. 2 und ihr Art. 6, ist dahin auszulegen, dass sie einzelstaatlichen Rechtsvorschriften entgegensteht, die als Verarbeitungszweck der PNR-Daten die Beaufsichtigung bestimmter Aktivitäten der Nachrichten- und Sicherheitsdienste zulassen, soweit die nationale PNR-Zentralstelle im Rahmen eines solchen Zwecks gehalten wäre, die Daten zu verarbeiten und/oder sie oder die Ergebnisse ihrer Verarbeitung zu anderen als den in Art. 1 Abs. 2 dieser Richtlinie erschöpfend aufgeführten Zwecken an die erwähnten Dienste zu übermitteln, was das nationale Gericht zu prüfen hat.

11. Art. 12 Abs. 3 Buchst. b der Richtlinie 2016/681 ist dahin auszulegen, dass die PNR-Zentralstelle keine „andere zuständige nationale Behörde“ im Sinne dieser Vorschrift darstellt.

12. Art. 3 Abs. 1 der Richtlinie 2004/82, wonach die Mitgliedstaaten die erforderlichen Schritte unternehmen, um die Fluggesellschaften zu verpflichten, auf Anfrage der mit der Durchführung der Personenkontrollen an den Außengrenzen beauftragten Behörden bei Abschluss des Check-in die Angaben über die in Abs. 2 in Verbindung mit Art. 2 Buchst. b und d dieser Richtlinie genannten Personen zu übermitteln, betrifft nur Personen, die zu einer für das Überschreiten der Außengrenzen der Mitgliedstaaten zu Drittstaaten zugelassenen Grenzübergangsstelle befördert werden. Einzelstaatliche Rechtsvorschriften, die diese Verpflichtung mit dem alleinigen Ziel der Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung auf die Daten von Personen ausdehnen würden, die mit dem Flugzeug oder mit anderen Verkehrsmitteln die Binnengrenzen des betreffenden Mitgliedstaats überschreiten, würden gegen Art. 67 Abs. 2 AEUV und Art. 22 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Unionskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) verstoßen.

13. Ein nationales Gericht kann eine Bestimmung seines nationalen Rechts, die es ermächtigt, die zeitliche Wirkung einer ihm nach diesem Recht obliegenden Feststellung der Rechtswidrigkeit zu beschränken, nicht auf einzelstaatliche Rechtsvorschriften anwenden, die Luft-, Land- und Seebeförderungs- sowie Reiseunternehmen im Hinblick auf die Bekämpfung von Terrorismus und schwerer Kriminalität zu einer Übermittlung von PNR-Daten verpflichten und eine mit den Art. 7, 8 und 52 Abs. 1 der Charta der Grundrechte unvereinbare allgemeine und unterschiedslose Verarbeitung und Vorratsspeicherung dieser Daten vorsehen. Nach dem Effektivitätsgrundsatz ist ein nationales Strafgericht verpflichtet, Informationen und Beweise, die gemäß solchen mit dem Unionsrecht unvereinbaren Rechtsvorschriften erlangt wurden, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, terroristische Handlungen oder schwere Straftaten begangen zu haben, auszuschließen, wenn diese Personen nicht in der Lage sind, sachgerecht zu diesen Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen.